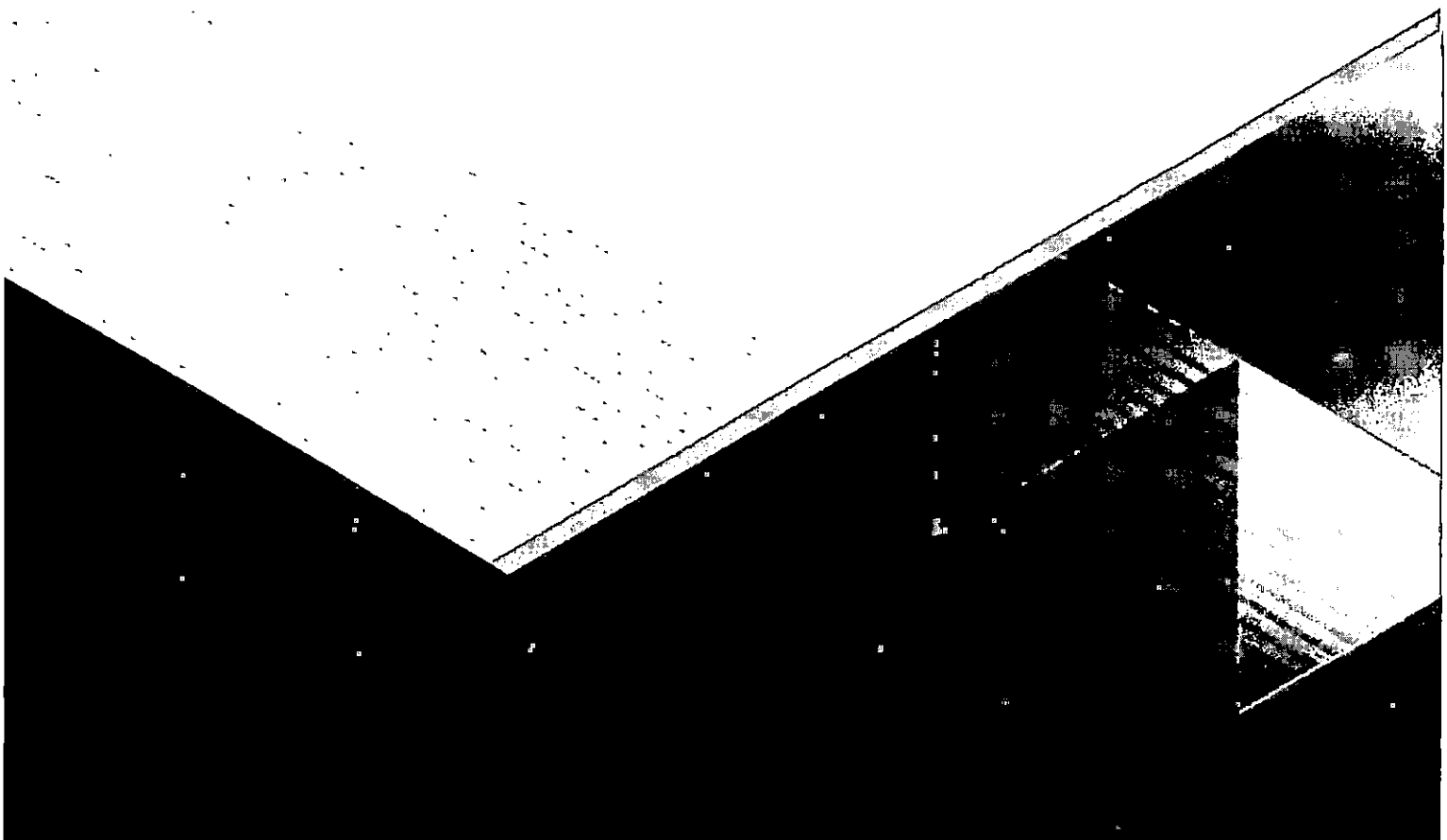
Banjercito

Crecemos con una misión: tu bienestar

SISTEMA DE GESTIÓN

BANCO NACIONAL DEL EJÉRCITO, FUERZA AÉREA Y ARMADA, S.N.C.



ÍNDICE

I. Introducción

De conformidad con el artículo 34 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (En adelante LGPDPPSO), el cual establece que las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un *sistema de gestión*, de igual forma el artículo 65 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (En adelante Lineamientos Generales) estipula que el *sistema de gestión* deberá permitir planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad.

Al respecto, el Oficial de Protección de Datos Personales de Banjercito, en cumplimiento a lo anterior, se avocó a la elaboración del presente **Sistema de Gestión de Seguridad de los Datos Personales**, mismo que sometió a aprobación del Comité de Transparencia, de conformidad con el artículo 83, segundo párrafo y 84, fracción I, de la LGPDPPSO, en su calidad de autoridad máxima en materia de protección de datos personales, contando con la atribución de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales

Conforme a lo expuesto el presente **Sistema de Gestión de Seguridad de los datos personales de Banjercito**, enmarca el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público, para la protección de los datos personales y los procesos de tratamiento de los mismos al interior del Banco Nacional del Ejército (En adelante Banjercito), a efecto de garantizar la privacidad de la información de nuestros usuarios, clientes, empleados, ex empleados, familiares de empleados y ex empleados, beneficiarios de empleados y ex empleados y proveedores.

II. Ámbito de aplicación

El presente **Sistema de Gestión de Seguridad de los datos personales de Banjercito**; es aplicable y de observancia obligatoria para todas las Unidades Administrativas, personal activo y prestadores de servicios y/o proveedores del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C., sea cual fuere su nivel jerárquico y su situación en la Institución; así como, para las personas externas que, debido a la prestación de un servicio, tengan acceso a tales sistemas o al sitio donde se ubican los mismos.

Cabe mencionar que la obligación de confidencialidad, debe subsistir aún después de que los involucrados hayan finalizado su participación en el tratamiento de datos personales porque hayan cambiado de funciones y aun cuando la relación laboral con esta Sociedad Nacional de Crédito haya concluido.

III. Definiciones

Ley General de Datos: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Responsable: Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C (En adelante Banjercito)

Encargado. La persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Alta Dirección de Banjercito. Toda persona con poder legal de toma de decisión en las políticas de la organización.

Activo. La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la organización.

Bases de datos. El conjunto ordenado de datos personales referentes a una persona física identificada o identificable.

Custodios. Son aquéllos con responsabilidad funcional sobre los activos, como: los responsables del departamento de datos, administradores de sistemas o responsables de un proceso o de un proyecto en específico, entre otros.

Datos personales. Cualquier información concerniente a una persona física identificada o identificable.

Incidente. Escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades.

Amenaza. Circunstancia o evento con la capacidad de causar daño a una organización.

Vulnerabilidad. Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

Riesgo. Combinación de la probabilidad de un evento y su consecuencia desfavorable.

Bases de datos. Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Bloqueo. La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

Borrado Criptográfico. Método de eliminación en el cual, la Llave de Cifrado del Medio (Media Encryption Key – MEK) utilizada para el cifrado de los datos (Key Encryption Key – KEK) es eliminada, haciendo que los datos cifrados con esa llave no puedan ser recuperados.

Catálogo de Disposición Documental: Registro general y sistemático que establece el plazo de conservación de las series documentales, tanto en archivos de trámite como en el archivo de concentración.

CD-RW. Disco Compacto de Lectura/Escritura. Puede aplicarse método de eliminación por purga y reescritura.

Supresión: Es la baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los mismos bajo las medidas de seguridad previamente establecidas por el responsable.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Aviso de privacidad: Documento a disposición del titular de los datos personales, generado por el responsable, de forma física, electrónica o en cualquier formato, previo a la recabación y tratamiento de sus datos, con el objeto de informarle sobre la finalidad del tratamiento, los datos recabados, así como la posibilidad de acceder, rectificar, oponerse o cancelar el tratamiento de los mismos.

Ciclo de vida: Tiempo que duración y conclusión del tratamiento de los datos personales, para después ser suprimidos, cancelados o destruidos por parte del responsable.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona física es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información como puede ser nombre, número de identificación, datos de localización, identificador en línea o uno o varios elementos de la identidad física, fisiológica, genética, psíquica, patrimonial, económica, cultural o social de la persona.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, información biométrica, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Finalidad: Los datos personales recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados. Los datos personales con fines de archivo de interés público, investigación científica e histórica, o estadísticos no se considerarán incompatibles con la finalidad inicial.

Instituto: Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI)

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales y los sistemas de datos personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se consideran las siguientes actividades:
a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados [illegible]

tratamiento; de manera enunciativa más no limitativa, se consideran las siguientes actividades:
a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Sistema de Datos Personales: Conjunto de organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de los sujetos obligados, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

Titular: La persona física a quien corresponden los Datos Personales.

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.
Tratamiento: Cualquier operación o conjunto de operaciones efectuadas sobre datos personales o conjunto de datos personales, mediante procedimientos manuales o automatizados relacionadas con la obtención, uso, registro, organización, estructuración, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión o cualquier otra forma de habilitación de acceso, cotejo, interconexión, manejo, aprovechamiento, divulgación, transferencia, supresión, destrucción o disposición de datos personales.

Unidad de Transparencia: Instancia que auxilia, orienta, gestiona, establece, informa, propone, aplica, asesora, registra y realiza las gestiones necesarias para el manejo, mantenimiento, seguridad, y protección de los sistemas de datos personales en posesión del responsable.
Usuario: Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas de datos personales.

IV. Políticas internas para la gestión y tratamiento de datos personales

En todo tratamiento de datos personales que se realice en Banjercito, se deberán respetar los principios y deberes dispuestos en la LGPDPPSO, asimismo, se deberá privilegiar el interés superior del niño, niña y adolescente, quedando prohibidos los tratamientos que tengan como efecto cualquier tipo de discriminación.

Lo anterior, en los términos que se explican a continuación:

Cumplimiento de los principios de licitud, finalidad, consentimiento, lealtad, calidad, proporcionalidad, información y responsabilidad mandatados por la Ley General de Protección

El tratamiento de los datos personales que estos realicen deberá sujetarse a las facultades o atribuciones que la normativa aplicable les confiera. **(Principio de licitud)**

Banjercito está obligada a tratar los datos personales privilegiando la confianza que deposita el titular en el responsable, respecto de que los datos personales proporcionados serán tratados conforme a lo que acordaron, así como a lo señalado por la normatividad y el aviso de privacidad correspondiente. **(Principio de lealtad)**

Banjercito, tiene la obligación de comunicar al titular de los datos personales, las características principales del tratamiento al que será sometida su información personal, así como los medios para ejercer sus derechos ARCO, lo que se materializa a través del Aviso de Privacidad**. (Principio de información)**

Principio de consentimiento: Banjercito deberá contar con el consentimiento del titular para el tratamiento de sus datos personales. Adicionalmente, la obtención del consentimiento deberá reunir las siguientes características:

- **Libre:** Que no medie error, mala fe, violencia o dolo que puedan afectar la manifestación de la voluntad del titular.
- **Específico**: Que refiera a una o varias finalidades determinadas que justifiquen el tratamiento de los datos personales.
- **Informado:** Que el titular tenga el conocimiento del aviso de privacidad previo al tratamiento al que serán sometidos sus datos personales y que conozca las consecuencias de otorgar su consentimiento.

Los datos personales sólo pueden ser tratados para cumplir con la(s) finalidad(es) que hayan sido informados al titular en el aviso de privacidad y, en su caso, consentidas por éste, o bien, para aquellas finalidades que sean compatibles o análogas. **(Principio de finalidad)**

Sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido y que se encuentren previstas en el aviso de privacidad. **(Principio de proporcionalidad)**

Principio de calidad: Conforme a la finalidad (es) para las que se vayan a tratar los datos personales, éstos sean:

- **Exactos:** Cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles.
- **Completos:** Cuando no falta ningún dato personal que se requiera para las finalidades para las que se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular.
- **Actualizados:** Cuando los datos están al día y corresponden a la situación presente del titular.
- **Correctos:** Cuando los datos personales no tienen errores o defectos y por ello cumplen con todas las características previas, es decir, son exactos, completos, pertinentes y actualizados.

Banjercito deberá asegurar el cumplimiento de los principios de protección de datos personales, con relación a los datos que se encuentren bajo su custodia o posesión, o bien, aquellos que haya comunicado un encargado, así como rendir cuentas de su tratamiento. **(Principio de responsabilidad)**

Deber de seguridad y confidencialidad

Los deberes que aplican y que se deben observar para el tratamiento de los datos personales son el de **seguridad** y el de **confidencialidad**; el primero, implica que Banjercito debe establecer y mantener medidas de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión; mientras que derivado del deber de **confidencialidad**, se deben definir controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

El **artículo 31 de la LGPDPPSO** establece que, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable (Banjercito) tendrá el deber de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan:

· Protegerlos contra pérdida, destrucción, robo, extravío, copia, uso, acceso, tratamiento, daño, alteración o modificación no autorizado, a través de medidas de seguridad administrativas, físicas y técnicas, las cuales constaran en un Documento de Seguridad, todo ello con la finalidad de conservar su confidencialidad, integridad y disponibilidad.

En ese sentido, el **artículo 35 de la LGPDPPSO**, dispone la descripción de manera particular de dichas medidas a través de la elaboración de un **Documento de Seguridad**.

V. Medidas de seguridad para la protección de los datos personales

Las medidas de seguridad de los datos personales son el conjunto de acciones, actividades, controles o mecanismos que permiten protegerlos contra su daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, garantizando con ello su confidencialidad, integridad y disponibilidad.

Las medidas de seguridad pueden clasificarse en administrativas, físicas y técnicas, las cuales de conformidad con el artículo 3, fracciones XXI, XXII y XXIII de la LPDPPSO, se refieren a lo siguiente:

1. Medidas de seguridad administrativas: políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal.

2. Medidas de seguridad físicas: conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se consideran las actividades siguientes:

- Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
-Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; y,
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

3. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con *hardware* y *software* para proteger el entorno digital de los datos personales y los recursos involucrados en su

tratamiento. De manera enunciativa más no limitativa, se considerar las actividades siguientes:
- Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del *software* y *hardware*; y,
- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Analizando dichas declaraciones, en conjunto con las acciones y mecanismos que Banjercito mantiene para asegurar su función y el cumplimiento de sus atribuciones; se procede a enunciar, de manera general, las medidas de seguridad de los datos personales.

Medidas de seguridad administrativas.

1. Manual General de Organización de Banjercito, con última fecha de actualización 01 de junio de 2020; herramienta técnico-administrativa de observancia general y obligatoria para todo el personal de Banjercito que establece las funciones y responsabilidades de las Unidades Administrativas que lo conforman, de acuerdo con sus competencias.

2. Programa General de Capacitación en Materia de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual concentra los objetivos, ejes temáticos y programas que deberán implementarse para el cumplimiento de las atribuciones y principios relacionados con la capacitación y actualización de los servidores públicos de los órganos y unidades administrativas del CJF en las materias indicadas. 6. Las establecidas para el cumplimiento de los principios, deberes y políticas de protección de datos personales en el Sistema de Gestión de Seguridad de Datos Personales y Programa General de Datos Personales.

Medidas de seguridad físicas.

Aquellas establecidas por la Subdirección de Seguridad y la Subdirección de Seguridad de la Información, para preservar la seguridad de los servidores públicos, instalaciones, equipos y demás bienes de Banjercito, las cuales se encuentran documentadas en el Manual de Políticas y Procedimientos para la protección y seguridad de Banjercito y el Manual de Políticas y Procedimientos de Seguridad de la Información

- Medidas adicionales a las Medidas Básicas de Seguridad.
- Excepciones para implantar medidas de seguridad.
- Procedimiento para determinar el porcentaje de siniestralidad para efectos de excepción.
- Medidas de Seguridad Informática.
- Disposiciones de seguridad informática.
- Seguridad física de las instalaciones donde residan los equipos de cómputo y telecomunicaciones de las Sucursales.
- Seguridad lógica de las redes de datos, aplicaciones y telecomunicaciones.
- Seguridad en redes de datos.
- Aplicaciones.
- Telecomunicaciones.
- Controles en el procesamiento de datos, sistemas, programas y medios automatizados.
- Seguridad en la información no automatizada.
- Manejo de información confidencial.
- Sistemas de monitoreo y alarma de transmisión de datos de seguridad, y de video grabación de imágenes.
- Proceso de emisión, transmisión y recepción de Señales de Alarma.
- Diagrama del Sistema de Monitoreo y Alarma.
- Coordinación con autoridades militares y civiles en caso de una eventualidad.
- Activación remota de la Señal de alarma.
- Activación de la Señal de alarma a través del Money clip en ventanillas.
- Aplicación interface para activación de la Señal de alarma.
- Sistema de comunicaciones de datos de seguridad.
- Sistema de videograbación de imágenes de seguridad.
- Funciones del sistema de videograbación de imágenes de seguridad.
- Proceso de grabación de señales y disponibilidad de imágenes durante Siniestros o Conductas Ilícitas.
- Colocación de las cámaras del circuito cerrado de televisión.
- Lineamientos para la destrucción de las videocasetes utilizados en el Sistema de Circuito Cerrado de Televisión.
- Especificaciones técnicas mínimas de los sistemas.
- Dispositivos y mecanismos de respaldo para los sistemas.
- Prestadores de servicios.
- Empresas de mantenimiento.

- Empresas de limpieza.
- Programa de Seguridad y Protección.
- Políticas y sistemas institucionales de operación relativos a la Seguridad y Protección.
- Lineamientos para el reclutamiento, selección, capacitación y evaluación del personal, en materia de Seguridad y Protección.
- Lineamientos para el reclutamiento y selección de personal.
- Seguridad y Acceso a Instalaciones.
- Seguridad para el Acceso a las Instalaciones del Edificio Corporativo.
- Control de Credenciales de Acceso a Banjercito para Personal Externo.

Manual de Políticas y Procedimientos de Seguridad de la Información de Banjercito

- Políticas de seguridad física y ambiental
- Perímetro de seguridad física.
- Controles Físicos de entrada.
- Protección de oficinas e instalaciones.
- Protección contra amenazas externas y ambientales.
- Trabajo en áreas seguras
- Áreas de carga y descarga.
- Equipos.
- Servicio público de energía.
- Seguridad del cableado
- Mantenimiento de equipos.
- Retiro de los bienes.
- Seguridad de los equipos fuera de las instalaciones.
- Reutilización segura de los equipos.
- Equipos desatendidos en áreas de usuarios.
- Política de pantalla y escritorio limpio.
- Política particular para control de entrada de equipo de cómputo sin acceso a red.

Medidas de seguridad técnicas.

Las estipuladas por la Dirección de Tecnologías de la Información y Comunicaciones, la Subdirección de Seguridad de la Información y la Unidad de Transparencia, para impulsar la operación eficiente y la modernización en la automatización de los procesos necesarios para el ejercicio de las funciones del personal de Banjercito, a través de la generación de sistemas y administración de la infraestructura de cómputo.

Las previstas en el **Manual de Políticas y Procedimientos de seguridad de la información**, Manual **de Políticas y Procedimientos del Centro de Cómputo** y el **Manual de Políticas y Procedimientos de gestión y protección de datos personales:**

Manual de Políticas y Procedimientos de seguridad de la información

- Lineamientos para asegurar la confidencialidad, integridad y disponibilidad de la información.
- Contacto con autoridades
- Contacto con grupos de interés especial
- Política de dispositivos móviles
- Política de teletrabajo
- Política de seguridad de la información en recursos humanos antes, durante y una vez terminada la contratación.
- Políticas de gestión de activos.
- Responsabilidad sobre los activos.
- Clasificación de la información.
- Manejo de los soportes de almacenamiento
- Política para la eliminación de información en dispositivos de almacenamiento electrónico.
- Política para la administración de perfiles de seguridad de la información en equipos de cómputo.
- Política particular para administración y uso de dispositivos de almacenamiento.
- Política de control de accesos
- Utilización de los servicios de Red.
- Administración de los accesos de usuarios.
- Registro y bajas de usuarios.
- Identificación y autenticación de los usuarios.
- Administración de privilegios.
- Administración de contraseñas de usuarios.
- Revisión de derechos de accesos de usuarios.
- Retirada o adaptación de los derechos de acceso.
- Responsabilidades de los usuarios en el uso de contraseñas.
- Control de acceso a las aplicaciones.
- Política particular para mecanismos y controles robustos de acceso a la infraestructura.
- Política particular para control de acceso de usuarios a los sistemas corporativos.
- Política particular para el control de acceso a los sistemas de cómputo de Banjercito para los accesos no autorizados.

- Política particular para control de acceso a internet corporativo.
- Política particular para el servicio de correo electrónico institucional externo.
- Política particular para creación de nuevas cuentas de usuario en sistemas corporativos.
- Administración de redes.
- Procedimientos y responsabilidades operativas.
- Protección contra software malicioso.
- Política de respaldos de información.
- Registros y supervisión.
- Control de arranque del sistema operativo.
- Control del software operativ
- Gestión de vulnerabilidad técnica.
- Restricciones en la instalación de software.
- Controles de auditorías de sistemas de información.
- Subproceso de configuración de las herramientas para detectar virus.
- Subproceso de identificación de código malicioso.
- Política particular para investigación y monitoreo de nuevas vulnerabilidades en infraestructura tecnológica.
- Política particular equipo de cómputo no pertenecientes a Banjercito y que requieran acceso a red corporativa.
- Política particular para la entrada y salida de equipo de cómputo portátil que es propiedad de Banjercito y que fue asignado a empleados.
- Política particular para control de salida de equipo de cómputo con acceso a red.
- Política particular para dar de baja equipo de cómputo.
- Política particular para auditar los sistemas de información de Banjercito.
- Política particular para realizar el escaneo de vulnerabilidades y pruebas de penetración en tecnologías de la información en producción.
- Política particular para revisar vulnerabilidades en tecnologías de la información en ambiente de desarrollo.
- Política particular para verificación de código malicioso en dispositivos de almacenamiento (USB, disco duro, DVD, CD, etc.).
- Mecanismos de seguridad asociados a servicios en red.
- Intercambio de información
- Convenio de confidencialidad
- Política particular para la gestión de la red de telecomunicaciones.
- Subproceso de resguardo del diagrama de conexión de la red de Banjercito.
- Subproceso de segmentación de red de Banjercito.
- Subproceso de cifrado para la Interconexión entre los centros de datos.

- Subproceso de cifrado para la administración de los equipos de telecomunicaciones.
- Subproceso de mecanismos de autenticación, autorización y registro para la administración de los equipos de telecomunicaciones.
- Subproceso de configuración de NTP en los equipos de telecomunicaciones. Subproceso de monitoreo de los equipos de telecomunicaciones.
- Subproceso de habilitación de bitácora local de eventos en equipos de telecomunicaciones.
- Política particular para restricción de uso de protocolos inseguros en la infraestructura tecnológica de Banjercito.
- Política particular para el uso de redes inalámbricas. Requerimientos de seguridad de los sistemas.
- Seguridad en el desarrollo y en los procesos de soporte.
- Requerimientos de seguridad en contratos de tercerización.
- Cadena de suministro en tecnologías de la información y comunicaciones.
- Gestión de la prestación de servicios por proveedores.
- Supervisión y revisión de los servicios prestados por terceros y/o comisionistas.
- Gestión de cambios en los servicios prestados por terceros y/o comisionistas.
- Responsabilidad y procedimientos para administrar incidentes de seguridad.
- Reporte de incidentes de seguridad.
- Reporte de incidentes de seguridad a autoridades.
- Notificación de puntos débiles de seguridad.
- Valoración de eventos de seguridad de la información y toma de decisiones.
- Respuesta de incidentes de seguridad.
- Aprendizaje de los incidentes de seguridad.
- Recolección de evidencia.
- Planeación de la continuidad de la seguridad de la información.
- Seguridad de la información en la continuidad de negocio.
- Protección de los registros de Banjercito.
- Protección de datos y privacidad de la información personal.
- Regulación de controles para el uso de criptografía.
- Revisión de la seguridad de la información.
- Valoración de los activos por sus propiedades de seguridad.
- Valoración del impacto.
- Valoración de la probabilidad.
- Identificación de escenarios riesgo.

- Análisis de riesgos.
- Evaluación de riesgos.
- Tratamiento del riesgo, niveles de tolerancia y apetito de riesgo.
- Criterios de escalación en el tratamiento de riesgos.
- Riesgo residual.
- Monitoreo del riesgo.
- Revisión del riesgo.
- Informe de análisis y evaluación de riesgos.

Manual de Políticas y Procedimientos del Centro de Cómputo

- Atender solicitudes de altas y modificaciones de acceso al sistema para usuarios(as)
- internos.
- Atender solicitudes de altas y modificaciones de acceso al sistema para usuarios(as)
- externos.
- Acceso al sistema SIBA cuando un usuario(a) es promovido.
- Reactivar en caso de bloqueo por ingresar contraseña incorrecta.
- Cambiar contraseña por olvido.
- Atender solicitud de baja definitiva de las cuentas de usuario(a) del sistema SIBA.
- Realizar nuevo respaldo o recuperación de información.
- Atender procesos y/o reprocesos internos.
- Atender requerimientos de nuevo proceso de información.
- Atender requerimientos de usuarios(as) en instalación, configuración y fallas técnicas en sistemas, servidores y líneas de comunicación.
- Acceso a SIBA de usuarios(as) en periodo de incapacidad.
- Acceso al sistema SIBA de Banjercito de los usuarios(as) que toman su periodo vacacional.
- Administrar la operación del turno.
- Llevar el control interno de recursos e información.
- Acceso al Centro de Cómputo.
- Administrar los respaldos del Centro de Cómputo.
- Controlar y administrar los equipos centrales del Centro de Cómputo.
- Controlar la entrada y salida de cintas magnéticas para el intercambio de información
- entre el Centro de Cómputo y el Site alterno.
- Desmagnetizar medios magnéticos.
- Actuar en caso de sismos e incendios.
- Actuar en caso de sabotaje.

- Actualización del Plan de recuperación en caso de desastres del Centro de Cómputo.
- Activación de Servicios del Centro de Cómputo Alterno para SIBA y Sistema de Tarjeta de Crédito.
- Baja del equipo del Centro de Cómputo por obsolescencia o deterioro.
- Atención a solicitudes de altas y/o modificaciones de equipos virtuales con Sistema Operativo Windows y/o Unix.
- Instalación de actualizaciones de software multiplataforma en servidores centrales de la Institución.
- Liberación a producción por mantenimiento al Sistema BDT.
- Actualización e implementación periódica de parches de seguridad en los activos relacionados con aplicativos de la Red Financiera.
- Atención del Requerimiento.
- Solicitud del usuario de acceso a sistema.
- Atender solicitudes de altas y modificaciones de acceso al sistema para usuarios(as) internos.
- Atender solicitudes de altas y modificaciones de acceso al sistema para usuarios(as) externos.
- Acceso al sistema SIBA cuando un usuario(a) es promovido.
- Reactivación y cambio de contraseñas.
- Reactivar en caso de bloqueo por ingresar contraseña incorrecta.
- Cambiar contraseña por olvido.
- Solicitud de baja de usuarios(as).
- Atender solicitud de baja definitiva de las cuentas de usuario(a) del sistema SIBA.
- Requerimientos de Información en respaldos y procesos.
- Realizar nuevo respaldo o recuperación de información.
- Atender procesos y/o reprocesos internos.
- Atender requerimientos de nuevo proceso de información.
- Atender requerimientos de usuarios(as) en instalación, configuración y fallas técnicas en sistemas, servidores y líneas de comunicación.
- Solicitud de accesos temporales.
- Administración del Centro de Cómputo.
- Administrar la operación del turno.
- Llevar el control interno de recursos e información.
- Acceso al Centro de Cómputo.
- Administrar los respaldos del Centro de Cómputo.
- Administración de equipos.
- Controlar y administrar los equipos centrales del Centro de Cómputo.
- Instalación de actualizaciones de software multiplataforma en servidores centrales de la Institución.

- Controlar la entrada y salida de cintas magnéticas para el intercambio de información entre el Centro de Cómputo y el Site alterno.
- Desmagnetizar medios magnéticos.
- Actuación en caso de contingencia.
- Actuar en caso de sismos e incendios.
- Actuar en caso de sabotaje.
- Actualización del Plan de recuperación en caso de desastres del Centro de Cómputo.
- Activación de Servicios del Centro de Cómputo Alterno para SIBA y Sistema de Tarjeta de Crédito.
- Baja del equipo del Centro de Cómputo por obsolescencia o deterioro.
- Atención a solicitudes de altas y/o modificaciones de equipos virtuales con Sistema Operativo Windows y/o Unix.
- Instalación de actualizaciones de software multiplataforma en servidores centrales de la Institución.
- Liberación a producción por mantenimiento al Sistema BDT.
- Actualización e implementación periódica de parches de seguridad en los activos relacionados con aplicativos de la Red Financiera.

Manual de Políticas y Procedimientos para el manejo y protección de datos personales.

- Procedimiento para la atención de solicitudes de ejercicio de derechos ARCO
- Procedimiento de recepción y atención de dudas y/o quejas por parte de las/los titulares de datos personales.
- Programa de capacitación y actualización en materia de transparencia, acceso a la información pública, protección de datos personales y temas relacionados.
- Principios y deberes en materia de protección de datos personales
- Procedimiento de atención a incidentes de seguridad de la información que impliquen una vulneración a la seguridad de los datos personales.
- Procedimiento para la elaboración de avisos de privacidad.
- Auditoría en materia de protección de datos personales.

VI. Mecanismos y medios para la elaboración y difusión de Avisos de Privacidad

El Aviso de Privacidad será elaborado por el área dueña del proceso que corresponda mediante el cual se de tratamiento a los datos personales, en conjunto con el Jefe(a) de Departamento de Protección de Datos Personales y deberá ser remitido vía oficio a la Unidad de Transparencia, para que por su conducto sea sometido a estudio y en su caso aprobación por parte del Comité de Transparencia.

El oficio deberá ir acompañado del proyecto de aviso de privacidad en ambas modalidades (simplificado e integral), debidamente firmado por los titulares de las áreas involucradas o competentes que el Jefe(a) de Departamento de Protección de Datos Personales considere necesarias.

Contenido del aviso de privacidad.

El Aviso de privacidad deberá caracterizarse por ser sencillo, con la información necesaria, expresado en lenguaje corto y comprensible y con una estructura y diseño que facilite su entendimiento, atendiendo al perfil de las/los titulares de los datos personales a quien irá dirigido, con la finalidad de que sea un mecanismo de información práctico y eficiente, esto implica lo siguiente:

- No usar frases inexactas, ambiguas o vagas, como "entre otros", "como por ejemplo" o "de manera enunciativa más no limitativa".
- Redactar el aviso de privacidad en función del perfil de las/los titulares o público a quien va dirigido.
- No incluir textos o frases que induzcan a la/el titular, de manera engañosa o fraudulenta, a seleccionar una opción en específico.
- No incluir casillas u otros mecanismos similares que estén marcados previamente, que obliguen a las/los titulares a desmarcarlos para modificar la condición ahí establecida.
- No remitir al titular a textos o documentos que no estén disponibles, por ejemplo, a hipervínculos deshabilitados o que no contengan la información señalada.

Con base en el artículo 27 de la LGPDPPSO, el aviso de privacidad simplificado deberá contener la siguiente información:

- La denominación completa de Banjercito.
- Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento de la/el titular (finalidades primarias y secundarias).
- se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:
- Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno, así como las personas físicas o morales a las que se transfieren los datos personales.
- Las finalidades de estas transferencias.

Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para

finalidades y transferencias de datos personales que requieran su consentimiento.

- El sitio donde se podrá consultar el aviso de privacidad integral.
- Con base en el artículo 28 de la LGPDPPSO, el aviso de privacidad Integral debe contener la siguiente información:
- La identidad y domicilio del responsable.
- Las finalidades del tratamiento.
- Los mecanismos para que la/el titular pueda manifestar su negativa para finalidades secundarias o accesorias.
- Los datos personales tratados
- El señalamiento expreso de los datos personales sensibles que se traten.
- El fundamento legal que faculta al responsable para llevar a cabo el tratamiento.
- Las transferencias de datos personales que en su caso se efectúen.
- La cláusula que indique si el titular acepta o no la transferencia cuando así se requiera.
- Los medios y el procedimiento para ejercer los derechos ARCO.
- Los mecanismos y procedimientos para que, en su caso, la/el titular pueda revocar su consentimiento al tratamiento de sus datos personales.
- Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de sus datos personales.
- El uso de cookies, web beacons y/o cualquier otra tecnología similar o análoga.
- Portabilidad de datos.
- El domicilio de la Unidad de Transparencia
- Los procedimientos y medios por los cuales el responsable comunicará a las/los titulares los cambios en el aviso de privacidad.

Consentimiento para el tratamiento de datos personales.

El consentimiento es la manifestación de la voluntad libre, especifica e informada de la/el titular de los datos mediante la cual se efectúa el tratamiento de estos, misma que puede ser de manera expresa cuando la/el titular externa su voluntad por escrito, firma electrónica, medios ópticos o cualquier otra tecnología, que implique certeza de su identificación, o bien tácita cuando la/el titular no manifiesta oposición alguna, respecto al aviso de privacidad.

Banjercito no está obligado a recabar el consentimiento de la/el titular para el tratamiento de sus datos personales en los siguientes casos:

- Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en la presente normatividad, en ningún caso, podrán contravenirla.
- Cuando las transferencias que se realicen entre responsables sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.
- Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente.
- Para el reconocimiento o defensa de derechos de la/el titular ante autoridad competente.
- Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre la/el titular y el responsable.
- Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes.
- Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria.
- Cuando los datos personales figuren en fuentes de acceso público.
- Cuando los datos personales se sometan a un procedimiento previo de disociación.
- Cuando la/el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

Publicación del aviso de privacidad.

- El aviso de privacidad una vez aprobado por parte del Comité de Transparencia de Banjercito, se pondrá a disposición de las/los titulares de los datos personales en ambas modalidades y será difundido mediante:
- Correo electrónico interno (#TransparenciaNews).
- Portal web de Banjercito en el apartado de Transparencia / Avisos de Privacidad: https://www.banjercito.com.mx/Transparencia_Focalizada/avisos_privacidad.html
- Póster y flyer informativo
- Cualquier otro medio electrónico y/o físico que para tales efectos disponga el Comité de Transparencia.

VII. Procedimiento para la atención de solicitudes de ejercicio de derechos ARCO.

En todo momento el titular de los datos personales o su representante podrán ejercer alguno de los derechos de acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, conocidos como derechos ARCO, en el entendido que cualquiera de los derechos ARCO no es requisito previo, ni impide el ejercicio de otro.

El ejercicio de los derechos ARCO es gratuito, salvo que deban realizarse cobro para recuperar los costos de reproducción, certificación o envío. La información deberá ser entregada sin costo, cuando implique la entrega de no más de 20 hojas simples y la Unidad de Transparencia, podrá exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular, siempre y cuando medie solicitud de por medio al momento de ingreso de la solicitud de ejercicio de derechos ARCO y resolución favorable por parte del Comité de Transparencia.

Para el ejercicio de los derechos ARCO, los titulares de los datos personales deberán requisitar la "Solicitud de derechos ARCO de Banjercito", la cual podrá obtenerse en formato electrónico a través de la página web institucional:

- http://www.banjercito.com.mx/Transparencia_Focalizada/datos_personales.html
- El titular y/o su representante deberá presentar ante la Unidad de Transparencia la "Solicitud de derechos ARCO Banjercito", disponible en formato electrónico a través de la página web institucional: http://www.banjercito.com.mx/Transparencia_Focalizada/datos_personales.html, debidamente requisitada y firmada. a través de alguno de los canales de recepción siguientes:
- De manera presencial ante la Unidad de Transparencia de Banjercito (UT), ubicada en Av. Industria Militar 1055, Col. Lomas de Sotelo. Alcaldía Miguel Hidalgo, Ciudad de México, C.P. 11200, teléfonos 56260500, 55579188, extensiones 2631 y 2193.
- De manera presencial en la Red de Sucursales de Banjercito al interior de la República Mexicana y/o zona metropolitana.
- De manera presencial en las Oficinas de Servicios Bancarios Fronterizos y/o Oficinas Consulares.
- Vía correo Electrónico: unidad_transparencia@banjercito.com.mx
- Plataforma Nacional de Transparencia en el apartado correspondiente a Banjercito y/o Fideicomiso Banjercito.

Las solicitudes deberán ser presentadas previa acreditación de su identidad, mediante identificación oficial vigente con fotografía, así como de su representante legal, en caso de que éste sea quien presente la solicitud, presentando el original para su cotejo.

Para el ejercicio de los derechos ARCO será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante. El ejercicio de los derechos ARCO por persona distinta a su titular o su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.

En el ejercicio de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, de conformidad con las leyes civiles, se estará a las reglas de representación dispuesta en la misma legislación.
Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos ARCO, siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto.
Es importante tener en cuenta que, para la representación de menores de edad, personas en estado de interdicción o incapacidad declarada por ley, o personas fallecidas, la personalidad del representante deberá quedar debidamente acreditada previo al ejercicio del derecho de que se trate y además se deberán aportar los siguientes documentos, según sea el caso:

Para solicitudes de ejercicio de derechos ARCO de datos personales de menores de edad: Si los padres ejercen la patria potestad y son los que presenten la solicitud:
- Documento que acredite la identidad de menor.
- Acta de nacimiento del menor.
- Identificación oficial del padre o de la madre, que pretenda ejercer el derecho.
- Carta en la que se manifieste, bajo protesta de decir verdad, que el padre o la madre es quien ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad.

Si una persona distinta a los padres es quien ejerce la patria potestad, y es quien presenta la solicitud:
- Documento que acredite la identidad de menor.
- Acta de nacimiento del menor.
- Documento legal que acredite la posesión de la patria potestad.

- Identificación oficial de quien presenta la solicitud y posee la patria potestad.
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad.

Cuando un tutor es quien ejerce la patria potestad:
- Documento que acredite la identidad de menor.
- Acta de nacimiento del menor.
- Documento legal que acredite la tutela.
- Identificación oficial del tutor.
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la tutela.

Para solicitudes de derechos ARCO de datos personales de personas en estado de interdicción o incapacidad legal:
- Documento que acredite la identidad del titular de los datos personales.
- Instrumento legal de designación del tutor.
- Identificación oficial del tutor.

Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la misma.
Para solicitudes de derechos ARCO de datos personales de personas fallecidas:
- Identificación oficial de la persona a quien pertenecían los datos personales
- Acta de defunción
- Documento(s) que acrediten el interés jurídico de quien pretende ejercer el derecho, y
- Documento de identificación oficial de quien solicita el ejercicio del derecho

Además de la información general antes señalada, dependiendo del derecho que desee ejercer, deberá incluir la siguiente información en la solicitud:

- Derecho de acceso: La modalidad en la que prefiere que se reproduzcan los datos personales solicitados.
- Derecho de rectificación: Las modificaciones que solicita que se realicen a los datos personales, así como aportar los documentos que sustenten la solicitud.
- Derecho de cancelación: Las causas que motivan la petición de que se eliminen los datos de los archivos, registros o bases de datos del responsable del tratamiento.
- Derecho de oposición: Las causas o la situación que lo llevan a solicitar que finalice el tratamiento de sus datos personales, así como el daño o perjuicio

que le causaría que dicho tratamiento continúe; o bien, deberá indicar las finalidades específicas respecto de las cuales desea ejercer este derecho.

Recepción y registro de las solicitudes en ejercicio de los derechos ARCO.

Es importante que tome en cuenta que, si la solicitud no cuenta con la información necesaria, Banjercito podrá solicitar la información faltante por medio de un requerimiento, el cual se deberá emitir en un plazo máximo de 5 días hábiles contados a partir del día siguiente de la presentación de la solicitud, y el titular de los datos personales, tendrá 10 días hábiles, después de recibir la prevención, para proporcionar la información requerida, pues de lo contrario se tendrá como no presentada su solicitud.

Una vez que la Unidad de Transparencia, verifique que la solicitud cumple con todos los requisitos, entregará un Acuse de recibo en el que conste la fecha de recepción de la misma.
La Unidad de Transparencia de Banjercito, turnará la solicitud al área que esta estime competente, la cual informará de la existencia de la información solicitada y remitirá su respuesta en un término no mayor a 5 días hábiles contados a partir del día siguiente de la recepción del oficio de turno.
El plazo referido en el párrafo anterior podrá ser ampliado por una sola vez hasta por 5 días hábiles cuando así lo justifiquen las circunstancias, y siempre y cuando se notifique a la Unidad de Transparencia dentro del plazo de respuesta.
En caso de que la información no obre en los archivos de la Unidad Administrativa de Banjercito a la que fue turnada, ésta lo comunicará en un plazo máximo de 24 horas. En el supuesto de que los datos personales de una solicitud obren en sus archivos y ésta considere improcedente la solicitud de acceso, rectificación, cancelación u oposición, se deberá comunicar mediante oficio a la Unidad de Transparencia de manera fundada y motivada en un plazo no mayor a 5 días hábiles.
1) Entrega de la respuesta a la persona solicitante.
En caso de que Banjercito determine que es procedente el acceso, la rectificación, la cancelación u oposición de los datos personales, le notificará al solicitante, sobre la procedencia de su petición, para que, dentro de los 10 días hábiles siguientes, acredite fehacientemente su identidad y en el caso de ser asistido por un representante su personalidad e identidad, y se proceda al acceso, rectificación, cancelación u oposición de los datos personales que correspondan.
2) Costos de reproducción y entrega del material.
La documentación deberá ser entregada sin costo, cuando implique la entrega de hasta veinte hojas simples.
En el caso de que se generen costos de reproducción una vez que el titular de los datos personales o en su caso el representante realice el pago generado por

petición, la Unidad de Transparencia lo comunicará al área respectiva para que lleve a cabo la reproducción de las copias simples y/o certificadas, a efecto de que en un plazo no mayor a tres días hábiles pueda recoger las mismas.
Si una vez notificados los costos, el titular de los datos personales o su representante, no realiza el pago dentro de los 30 días hábiles siguientes, operará la caducidad del trámite.
Adicionalmente, si el titular de los datos personales reitera su solicitud de acceso en un periodo menor a 12 meses, los costos no serán mayores a tres días de Salario Mínimo General Vigente en la Ciudad de México.
En caso de que el titular de los datos personales haya elegido la opción de consulta directa, este deberá ponerse en contacto con la Unidad de Transparencia, con el propósito de establecer una cita con la instancia competente y realizar dicha consulta.
En cualquier caso, la entrega en soporte impreso o el acceso directo a la información solicitada se realizará de forma personal al solicitante o a su representante legal.
3) Atención y seguimiento de los recursos de revisión interpuestos en contra de las respuestas de Banjercito a las solicitudes de ejercicio de derechos ARCO

La Unidad de Transparencia orientará al titular de los datos personales o a su representante, sobre su derecho de interponer el recurso de revisión, así como el modo de hacerlo, en el caso de inconformidad con la respuesta a una solicitud de ejercicio de derechos ARCO, en términos de lo establecido en el artículo 94 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

VIII. Catálogo de tratamiento de datos personales y sistemas de datos personales

El Catálogo de tratamiento de datos personales de Banjercito es el siguiente:

CAPTACIÓN
-Otorgamiento de Banje-Nómina
-Cuenta concentradora Banjercito
-Cuenta de cheques en M.N. y Dólares
-Cuenta Efectiva
-Cuenta Efectiva PQ
-Producto Básico
-Gana Ahorro en M.N. Personas Físicas
-Inversiones en M.N.

COLOCACIÓN

-Otorgamiento de préstamo quirografario personal militar activo
-Renovación de préstamo quirografario personal militar activo
-Otorgamiento de préstamo quirografario personal militar en situación de retiro
-Renovación de préstamo quirografario personal militar en situación de retiro
-Otorgamiento de préstamo quirografario pensionista
-Renovación de préstamo quirografario pensionista
-Credito Hipotecario Banje-casa
-Crédito de Liquidez con garantía hipotecaria personal militar activo
-Crédito de Liquidez con garantía hipotecaria personal militar en situación de retiro

SERVICIOS

-Proceso de reclutamiento y selección
-Proceso de administración de Fondos de Ahorro y de Trabajo
-Banjecel
-Banjetel
-Cajeros Automáticos
-Cheque certificado
-Cheque de Caja
-Cheque de ventanilla
-Orden de pago nacional
-Orden de pago internacional
-Pago a pensionados
-Servicio de Cajas de Seguridad
-Servicio de Banca Electrónica
-Sistema de Pagos Electrónicos Interbancarios (SPEI)
-Sistema de Pagos Interbancarias (SPID)

Los sistemas de datos personales son los siguientes:

1	Sistema Integral Bancario (SIBA)	Todas las Unidades Administrativas de Banjercito
2	Sistema IST-SWITCH	Dirección de Banca Electrónica
3	Sistema de pagos electrónicos interbancarios dólares (SPID) Enlace	Dirección de Tesorería y Operaciones Bancarias
4	Sistema de pagos electrónicos interbancarios (SPEI) Enlace	Dirección de Tesorería y Operaciones Bancarias
5	Sistema de Banca Electrónica	Dirección de Banca Electrónica
6	Sistema de Plataforma y ventanilla SOFT-M , Sockets y sistema de firmas	Dirección de Banca Comercial

7	Sistema de validación de nóminas (SISVALN)	Dirección de Banca Electrónica
8	Sistema de consultas de Comités de Crédito	Dirección de Crédito, Sucursales, Dirección de Banca Comercial y Banca Electrónica
9	Sistema de Tesorería Bancario (SITEB)	Dirección de Tesorería
10	Sistema de consultas de créditos (SISCC)	Dirección de Crédito
11	SIBUCB-BANJERCITO	Dirección de Tesoreria
12	Sistema de digitalización de Contratos (LASSER FICHE)	Dirección de Crédito
13	Sistema de evaluación de créditos (Tek origination)	Dirección de Crédito
14	Sistema de digitalización de solicitudes de crédito en sucursales (SHUFFLE)	Dirección de Banca Comercial/Gerencia de evaluación
15	IMAGE CHECK	Dirección de Banca Comercial/Gerencia de evaluación.
16	Sistema de Web fiduciario Efisoft	Dirección Juridica Fiduciaria
17	Sistema Administrativo de Mensajería (SISMEN)	Subdirección de Gestión Documental/Gerencia de Coordinación de Archivos
18	Sistema de Administración Integral de Riesgos (SAIR MATHEMATICA) (SAIR WEB)	Dirección de Administración Integral de Riesgos
19	Sistema Integral de asuntos jurídicos (SIAJ)	Dirección Jurídica Fiduciaria
20	Sistema de riesgo operacional (SPIRO)	Dirección de Administración Integral de Riesgos
21	Sistema Interactivo de Evaluaciones (SIE)	Dirección de Administración Integral de Riesgos
22	Sistema para el módulo de ingresos y egresos (MIET)	Dirección de Operaciones Bancarias
23	Sistema de conciliación bancaria (SICABAN)	Dirección de Operaciones Bancarias
24	Sistema IITV Internet	Dirección de Operaciones Bancarias Fronterizas
25	Sistema IITV	Dirección de Operaciones Bancarias Fronterizas

26	Pre validador NEPE (SAT)	Dirección de Operaciones Bancarias Fronterizas
27	Sistema de Registro de Requerimientos (SISEREN)	Dirección de Planeación y Seguimiento
28	Sistema de Gestión de Aclaraciones (SIGA)	Centro de atención a clientes
29	Sistema de Limpieza de Datos (SILD)	Centro de atención a clientes
30	CARDMAN	Dirección de Banca Electrónica
31	CA2	Dirección de Operaciones Bancarias
32	SMETF	Dirección de Administracion Integral de Riesgos
33	Sistema Integral de Recursos Humanos (SIRH)	Dirección de Factor Humano
34	Sistema de Conciliación de Cajeros Automáticos	Dirección de Operaciones Bancarias, Direccion de Banca Comercial/Gerencia de Tarjetas de Crédito
35	Sistema de Activo Fijo	Dirección de Administración Integral de Riesgos
36	Sistema de Administración de servicios de traslado de valores (SASTV)	Subdirección de Administración de Servicios Bancarios Fronterizos
34	Sistema de calificación de riesgos para PLD	Oficina de Cumplimiento
35	ALTAIR	Oficina de Cumplimiento
36	Módulo de Reportes de Operaciones Sospechosas de Clientes y Empleados	Oficina de Cumplimiento
37	TSYS PRIME	Oficina de Cumplimiento
38	Sistema ODWEK	Oficina de Cumplimiento
39	Monitor Plus-Analizadores Alertas y Workflow Simulador interfaces	Oficina de Cumplimiento
39	Sistema para la consulta de castigos y quebrantos (SPACCQ)	Dirección de Crédito

IX. Roles y responsabilidades en materia de protección de datos personales

Dirección General de Banjercito: Será la encargada de garantizar que se cumpla al interior de Banjercito las directrices del Sistema de Gestión de seguridad de los Datos Personales, dotando al Comité de Transparencia y Oficial del Protección de

Datos Personales de la legitimación correspondiente para su coordinación, supervisión, actualización y vigilancia.

Comité de Transparencia de Banjercito: Autoridad máxima en materia de protección de datos personales, encargado de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de datos personales en Banjercito.

Oficial de Protección de datos personales de Banjercito: Conforme al artículo 85 de la LGPDPPSO, será el encargado de asesorar a las unidades administrativas de Banjercito en materia de datos personales, así como, realizar el monitoreo y supervisión periódica (Anual) de las políticas, planes, procesos y procedimientos implementados en materia de tratamiento y protección de los datos personales, a fin de verificar el debido cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y, en su caso, proponer al Comité de Transparencia las mejoras de manera continua que estime necesarias.

Oficial en Jefe de Seguridad de la Información (CISO chief information security officer): Es el responsable en materia de seguridad de la información del Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C., y deberá responder a los requerimientos formulados por las autoridades y al interior de la Institución en cuestiones de seguridad de la información, de todos los sistemas del Banco, será el encargado de generar e implementar las políticas de privacidad y seguridad de la información, administrar el control de acceso a la información de Banjercito y supervisar el cumplimiento normativo de la seguridad de la información.

Propietarios de la información. Siempre será el Titular de la Unidad Administrativa donde se genere o posea la información, quien deberá identificar y comunicar al Oficial de Protección de Datos Personales de Banjercito los roles y responsabilidades específicas de los involucrados internos y externos dentro de su Unidad Administrativa, relacionados con los tratamientos de datos personales que se efectúen, el ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe, considerando su obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las cuales fueron recabados, así como la cadena de rendición de cuentas de todas las personas que traten datos personales al interior de su Unidad Administrativa, el catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales, finalidades de cada tratamiento, catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no, el nombre completo

denominación social del encargado de datos personales y de la formalización del **Anexo de Tratamiento de Datos Personales** para la prestación de servicios que brinda a Banjercito y los destinatarios o terceros receptores de las trasferencias que se efectúen, así como las finalidades que justifican éstas.

Grupo Estratégico de Seguridad de la Información (Dirección General, Dirección de Tecnologías de la Información y Comunicaciones, Subdirección de Seguridad de la Información, Dirección de Administración Integral de Riesgos, Titulares de las Unidades de Negocio, Invitados) : Órgano Colegiado responsable de proponer y aprobar, en conjunto con el Oficial de Protección de Datos Personales de Banjercito, entre otras las directrices en materia de seguridad de activos, organización de la seguridad de la información, establecimiento de controles internos y externos a través de los cuales se gestione la seguridad de activos. Considera, entre otros aspectos, la organización interna, que a su vez se refiere al compromiso de la alta dirección y la designación de responsables, entre otros objetivos; asimismo, considera aspectos externos como la identificación de riesgos relacionados con terceros, clasificación y control de activos, establecimiento de controles en materia de identificación, inventario, clasificación y valuación de activos conforme a la normatividad aplicable, seguridad relacionada a los recursos humanos, controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral, administración de incidentes de seguridad de la información, implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información, así como, las soluciones para la eliminación segura de los datos personales y la verificación de que la información no es recuperable, así como el establecimiento de las medidas de seguridad necesarias para el cumplimiento cotidiano de las políticas de gestión y tratamiento de datos personales.

Gerencia de Coordinación de Archivos. - Proporcionar asesoramiento en materia archivística y de protección de datos personales, de acuerdo a la normatividad aplicable a Banjercito, para la debida clasificación de la información, el bloqueo de los datos personales, y la cancelación (Eliminación o supresión definitiva) de los datos personales.

Dirección de Tecnologías de la Información: Unidad administrativa encargada de informar al Oficial de Protección de Datos Personales de manera anual, la descripción general de los sistemas de tratamiento de datos personales (sistemas interinstitucionales, aplicaciones o bases de datos con soporte electrónico), así como, el listado de los servidores públicos que tienen acceso a los sistemas de tratamiento de datos personales (sistemas interinstitucionales)

la ubicación física del equipo de cómputo del personal con acceso a sistemas interinstitucionales, así como del establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad implementadas.

Subdirección de Seguridad de la Información: Unidad administrativa encargada de la preservación de la confidencialidad, integridad y disponibilidad de la información de Banjercito, para que esta no esté a disposición o sea revelada a personas, entidades o procesos no autorizados (Confidencialidad), así como asegurar la propiedad de los activos del Banco, para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados (accesibilidad) y que los activos sean salvaguardados con exactitud y completitud (integridad). También será la encargada del establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad de la información relacionada con riesgos tecnológicos

Dirección de Administración Integral de Riesgos: Unidad Administrativa encargada del establecimiento de medidas para garantizar la continuidad de las operaciones, establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información, incluyendo la planeación, implementación, prueba y mejora del plan de continuidad de la operación de Banjercito, coadyuvando con el Oficial de Protección de Datos Personales de Banjercito, para que en caso de que se materialice una vulneración y/o riesgo y/o amenaza que afecte de forma significativa los derechos patrimoniales o morales de los titulares de datos personales se informe por los conductos oficiales al titular y al Instituto Nacional de Transparencia , Acceso a la Información y Protección de Datos Personales (INAI) y se implemente de manera inmediata un plan de trabajo de las acciones preventivas y correctivas para adecuar las medidas de seguridad y tratamiento de datos personales, a efecto de evitar que la vulneración se repita.

Subdirección de Seguridad Institucional: Unidad administrativa del establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad física y ambiental, así como el establecimiento de controles relacionados con los perímetros de seguridad física y entorno ambiental de los activos de Banjercito, con el fin de prevenir accesos no autorizados, pérdida o destrucción no autorizad, robo, extravío, daño, alteración de activos, entre otras amenazas, enfocándose en aspectos tales como los controles implementados para espacios seguros.

Unidades Administrativas de Banjercito: Por conducto de sus **enlaces de datos personales**, son las encargadas de identificar el método de almacenamiento seguro, guarda y custodia y eliminación segura de los datos personales, con base

en su clasificación, riesgo, tipo de medio, reutilización y si permanecerá o no Banjercito, así como de los procesos de bloqueo y cancelación, según lo indicado en el Cuadro General de Clasificación Archivística del Instituto y la normativa aplicable.

Responsable del Sistema de datos personales: Siempre será el Titular de la Unidad Administrativa donde se administre el Sistema de que se trate, quien deberá:

- Dar aviso al Oficial de Protección de Datos Personales de Banjercito, de los sistemas que involucren tratamiento de datos personales, a cargo de su Unidad.
- Designar al Administrador del Sistema Interinstitucional de que se trate.
- Validar la información entregada por los titulares de los datos personales, sea la estrictamente necesaria para cumplir con los fines legales para los cuales se hubieran recabado.

Administrador del Sistema de datos personales: Será el servidor público a quien designe de manera expresa el Titular de la Unidad Administrativa, estando a cargo la responsabilidad de la administración del sistema y de los operadores. Deberá**:**

- Mantener actualizado el Sistema
- Determinar los servidores públicos que deben tener acceso a los datos personales, en función del tratamiento que debe aplicarse a los mismos.
- Autorizar los accesos de los servidores públicos, determinar los privilegios y limitantes y llevar a cabo un registro de los mismos.
- Implementar las medidas de seguridad con la finalidad de evitar vulneraciones de la información.

Operador (es) del Sistema de datos personales: Servidores públicos de Banjercito que requieren de la autorización de los dueños de los responsables de los sistemas interinstitucionales, para accesar **a** la información y poder realizar su función a través de los recursos asignados apegándose a la normatividad existente. Por lo tanto, deben:

- Solicitar al responsable del sistema de datos personales de que se trate, el acceso a su información y sistemas.
- Abstenerse de utilizar información y/o sistemas si no cuenta con la debida autorización.
- Cumplir con los controles establecidos.
- Reportar errores y anomalías en la información o en los mecanismos de control.

- Reportar violaciones a los controles establecidos a la Subdirección de Seguridad de la Información y Oficial de Protección de Datos Personales de Banjercito.

Sus funciones quedan determinadas por el administrador del sistema, de acuerdo al perfil que se haya asignado al tratamiento de los datos personales de cada uno de los sistemas, a través de la **responsiva de acceso a sistemas** correspondiente.

Encargado de datos: Son personas físicas o morales, públicas o privadas, ajenas al Banco, que sólo o conjuntamente con otros, da tratamiento a datos personales a nombre y por cuenta de Banjercito, dichos usuarios(as) autorizados tendrán acceso a la información y a los recursos de Banjercito, no formarán parte de la Institución, pero serán contratados por la misma o tendrán alguna relación de negocio con él. (Proveedores, personal de instituciones gubernamentales, personal de prácticas profesionales, personal de servicio social, entre otros)

En caso de tratarse de prestadores de servicios, deberán formalizar el Anexo de Tratamiento de Datos Personales, en términos del artículo 59 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y registrar su actuar cotidiano de tratamiento de datos personales mediante una **Bitácora de transferencia y remisión de datos personales (BTRDP-BANJERCTO)** y **Bitácora de acceso a expedientes y uso cotidiano de datos personales (BAUCDP-BANJERCITO).**

X. Funciones y obligaciones y cadena de rendición de cuentas de las personas que traten datos personales.

Todo servidor público de Banjercito, que en el ejercicio de sus funciones obtenga, use, registre, organice, conserve, elabore, utilice, comunique, difunda, almacene, posea, maneje, aproveche, divulgue, transfiera o disponga de datos personales, está obligado a cumplir con las siguientes disposiciones:

Al momento de recabar los datos personales:

- Dar un uso responsable, desde el momento de su obtención. No utilizar medios engañosos o fraudulentos para la obtención de los datos personales, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.
- Poner a disposición el Aviso de Privacidad que corresponda, de tal manera que el titular de los datos personales pueda conocer las características principales del tratamiento al que serán sometidos y cómo podrá ejercer sus derechos ARCO.
- Obtener el consentimiento del titular para el tratamiento de sus datos personales, salvo las excepciones previstas en los artículos 22 y 70 de la

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

- Cuando se recaben datos personales sensibles, patrimoniales y financieros, el consentimiento del titular deberá ser expreso y por escrito. Fuera de los casos antes mencionados, como regla es válido el consentimiento tácito siempre y cuando se ponga a disposición de los titulares el Aviso de Privacidad que corresponda.
- Evitar la creación de bases de datos de carácter sensible, salvo que se justifique plenamente la necesidad del tratamiento para la consecución de finalidades legítimas y concretas relacionadas con las actividades de Banjercito.
- Recabar sólo aquellos datos personales que sean estrictamente necesarios para las finalidades para las que se obtienen.

Durante el manejo o utilización de los datos personales:

- Respetar la expectativa razonable de privacidad del titular de los datos personales.
- Limitar el tratamiento de los datos personales conforme a lo expuesto por el Aviso de Privacidad que corresponda y en los términos establecidos en la normatividad aplicable.
- Mantener los datos personales actualizados y correctos.
- Limitar el periodo de conservación de los datos personales al mínimo necesario.
- Implementar medidas de carácter administrativo, físico y técnico que garanticen la confidencialidad e integridad de los datos personales.
- Informar al titular de los datos personales, en caso de presentarse un incidente de seguridad de la información en el que exista una vulneración ocurrida en cualquier fase del tratamiento que afecte de forma significativa derechos patrimoniales o morales de éste, en cuanto se confirme la vulneración sucedida por el Comité de Transparencia.
- Rendir cuentas al titular en caso de algún incumplimiento con relación a la protección de sus datos personales.

Una vez agotadas las finalidades que justificaron el tratamiento de los datos personales:

- Llevar a cabo la cancelación (Eliminación o supresión definitiva) de los datos personales cuando hayan concluido las finalidades que justificaron el tratamiento de los datos personales, previo bloqueo.

De manera general todo el personal de Banjercito debe garantizar la implementación de los siguientes hábitos en materia de protección de datos personales:

- Mantener su área de trabajo sin documentos y/o dispositivos de almacenamiento electrónico a la vista.
- Cerrar los cajones y resguardar la información clasificada como reservada y confidencial bajo su custodia en archiveros bajo llave.
- Evitar dejar los documentos que ya no sean utilizados sobre impresoras, escáneres o copiadoras.
- No utilizar hojas recicladas en caso de contener información sensible.
- Realizar la eliminación segura de información en equipos de cómputo, celulares, tabletas y medios de almacenamiento electrónico.
- Fijar periodos para la retención y destrucción de la información personal que se maneja.
- Fomentar una cultura de la seguridad de la información.
- Realizar respaldos periódicos de los datos personales.
- Utilizar cerraduras y candados para resguardar los datos personales.
- Bloquear o suspender la sesión en equipos de cómputo y dispositivos móviles cuando dejas de usarlos.
- Validar el destinatario de una comunicación antes de realizarla.

XI. Niveles de protección de los datos personales

En Banjercito se da tratamiento a las siguientes categorías de datos personales:

Categorías	Tipo de datos personales
Datos identificativos	El nombre, domicilio, teléfono particular, teléfono celular, firma, clave de Registro Federal de Contribuyente (RFC),Clave Única de Registro de Población (CURP), Clave de Elector, Matrícula de Servicio Militar Nacional, Número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, y demás análogos;
Datos electrónicos	Las direcciones electrónicas, tales como correo electrónico no oficial, dirección IP(Protocolo de Internet), dirección MAC (Dirección de media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseña, firma electrónica; o cualquier otra información empleada por la persona, para su identificación en internet, acceso a sistemas de información u otra red de comunicaciones electrónicas;
Datos laborales	Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias

	personales, solicitud de empleo, hoja de servicio y demás análogos
Datos académicos	Trayectoria educativa, calificaciones, Títulos, Cédula profesional, certificados y reconocimientos y demás análogos;
Datos de salud	El expediente clínico de cualquier atención médica, referencias o descripción de sintomatología, detección de enfermedades incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona
Datos patrimoniales	Los correspondientes a bienes muebles o inmuebles, información fiscal, historial crediticio, ingresos o egresos, cuentas bancarias, seguros, fianzas servicios contratados, referencias personales y demás análogos
Datos sobre procedimientos administrativos	La información relativa a una persona que se encuentra sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho
Datos de tránsito y movimientos migratorios	Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria
Datos biométricos	Huellas dactilares, ADN, geometría de la mano, características de iris y retina y demás análogos
Datos sensibles	Origen étnico o racial, características morales o emocionales, ideologías y opiniones políticas, creencias, convicciones religiosas, filosóficas, la pertenencia a sindicatos, la salud y preferencia sexual
Datos personales de naturaleza pública	Aquellos que por mandato legal sean accesibles al público.

A efecto de realizar el análisis de riesgo correspondiente, se realizó la clasificación de los datos de acuerdo a su riesgo inherente conforme lo siguiente:

- **Riesgo inherente bajo**: Datos de identificación y contacto o información académica o laboral.

- **Riesgo inherente medio**: Datos que permiten conocer la ubicación física de la persona, tales como la dirección física, información relativa al tránsito

de las personas dentro y fuera del país, y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más.

También aquéllos que permitan inferir el patrimonio de una persona, datos de autenticación y cualquier otro que permita autenticar a una persona, datos jurídicos.

- **Riesgo inherente alto**: Datos personales sensibles, y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.

- **Riesgo inherente reforzado**: Los datos de mayor riesgo son los que de acuerdo a su naturaleza derivan en mayor beneficio para un atacante.

En general, los datos personales que maneja Banjercito, son de riesgo inherente alto.
Se identificaron los siguientes riesgos:

- Riesgo por tipo de dato.
- Riesgo por accesibilidad.
- Riesgo por nivel de anonimidad.

El **riesgo por tipo de dato** se calcula de acuerdo al beneficio que representa el obtener esta información para algún atacante.

Para tal efecto se toma en cuenta el nivel de riesgo inherente por cada tipo de dato que se trate y el volumen de titulares de cada dato tratado, agrupados de la siguiente manera:

Agrupador	Rango de Datos
<500	Datos de hasta 500 personas
<5k	Datos entre 501 hasta 5,000 personas
<50k	Datos entre 5,001 hasta 50,000 personas
<500k	Datos entre 50,001 hasta 500,000 personas
>500k	Datos de más de 500,000 personas

De acuerdo a lo anterior, se establecen cinco niveles de riesgo:

- Nivel 1-**Bajo:**
  - El nivel de riesgo inherente de los datos sea bajo, sin importar el número de personas.

- El nivel de riesgo inherente sea medio y se tengan hasta cinco mil (5,000) personas.
- El nivel de riesgo inherente sea alto y se tengan hasta quinientas (500) personas.

- Nivel 2-**Bajo medio**:
  - El nivel de riesgo inherente de los datos personales sea medio y se tengan hasta cincuenta mil (50,000) personas.
  - El nivel de riesgo inherente de los datos personales sea alto y se tengan hasta cinco mil (5,000) personas.

- Nivel 3-**Medio**:
  - El nivel de riesgo inherente de los datos personales sea medio y se tenga de cincuenta mil (50,000) personas en adelante.
  - El nivel de riesgo inherente de los datos personales sea alto y se tenga de cinco mil (5,000) personas en adelante.

- Nivel 4-**Medio alto**:
  - El nivel de riesgo inherente de los datos personales sea reforzado y se tengan hasta cinco mil (5000) personas.

- Nivel 5-**Alto**:
  - El nivel de riesgo inherente de los datos personales sea reforzado y se tengan más de cinco mil (5,000) personas.

Una vez establecidos dichos valores, se determinó que Banjercito cuenta con un riesgo por tipo de dato Medio bajo.

De manera general, de acuerdo al puntaje identificado en cada riesgo, se clasificarán de la siguiente manera:

Puntos	Riesgo
1	Bajo
2	Bajo medio
3	Medio
4	Medio alto
5	Alto

El **riesgo por accesibilidad** se establece determinando la cantidad de personas que tienen la posibilidad de accesar a los datos personales que protege la

Institución, en un periodo determinado. Entre mayor sea la accesibilidad, mayor es el riesgo para la información.

Agrupador Cantidad de accesos a los datos	Puntos por nivel de riesgo
≤ 20	1
>20 ≤ 200	2
> 200 ≤ 2,000	3
> 2,000	4

En el caso de Banjercito, dada la plantilla laboral con la que cuenta que se considera baja a comparación de otras Instituciones de crédito, y los controles establecidos por las áreas de seguridad relacionados con los permisos para ingresar a los sistemas de contienen datos personales, los cuales se otorgan de acuerdo al área de adscripción y a las funciones asignadas, no todos tienen las mismas facultades dentro de los sistemas, por lo que se reduce considerablemente el acceso a dichos sistemas, por lo que se tiene un riesgo por accesibilidad Medio bajo.

Una vez que se obtiene el Riesgo por accesibilidad, se debe de identificar que tan anónimos son los accesos a esta información, lo que se denomina **riesgo por tipo de entorno.** Esto representa la facilidad con la que podría ser identificado un atacante y los efectos negativos que tendrá, en caso de acceder o hacer un uso no autorizado de los datos tratados por Banjercito.

De acuerdo al entorno, se tienen los siguientes niveles de anonimidad, donde 1 implica baja anonimidad y 5 mayor anonimidad del atacante, es decir entre mayor anonimidad, mayor confianza tendrá el atacante para intentar vulnerar la seguridad.

Entorno	Nivel de Anonimidad
Físico	1
Red interna	2
Red inalámbrica	3
Red de terceros	4
Internet	5

Derivado de las políticas internas en materia de seguridad que maneja Banjercito, los únicos medios que se tienen para accesar a los sistemas institucionales, son a través de la red interna del Banco, quedando prohibido el

uso de medios de almacenamiento óptico, magnético o electrónico, sin que sean aprobados por la institución. Por lo anterior, se tiene un riesgo por nivel de accesibilidad Medio bajo.

De la combinación de los 3 riesgos analizados, se tiene como resultado un riesgo latente medio bajo para Banjercito.

A. SOLUCIONES PARA GARANTIZAR LA PROTECCIÓN DE DATOS.

Una vez establecido el nivel para cada uno de los riesgos establecidos, se identificaron las medidas de seguridad aplicables a Banjercito.

De acuerdo a lo establecido en la Metodología de Análisis de Riesgo BBA emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, de junio 2015, y con base en las listas y patrones de control que agrupan medidas de seguridad basadas en ISO/IEC27002, de acuerdo al riesgo por tipo de dato (Nivel 2) a Banjercito corresponde el uso de la siguiente tabla, en la cual las filas representan el nivel de anonimidad y las columnas el nivel de accesibilidad. En las celdas de dicha tabla se encuentran distribuidos los patrones de control y las listas de medidas de seguridad a implantar.

Riesgo por tipo de dato 2

		Medidas administrativas aplicables: AD-2			
Entornos de acceso	**Internet**	RI-1 DMZ-2 F-1	RI-1 DMZ-3 F-1	RI-2 DMZ-3 F-2	RI-2 DMZ-3 F-2
	Red Terceros	RI-1 DMZ-2 F-1	RI-1 DMZ-3 F-1	RI-2 DMZ-3 F-2	RI-2 DMZ-3 F-2
	WiFi	RI-1 DMZ-2 F-1	RI-1 DMZ-3 F-1	RI-2 DMZ-3 F-2	RI-2 DMZ-3 F-2
	Red Interna	RI-1 F-1	RI-1 F-1	RI-2 F-2	RI-2 F-2
	Físico	F-1	F-1	F-2	F-2
		≤ 20	**≤ 200**	**≤ 2,000**	**> 2,000**
		Cantidad de Accesos/Personas			

Las medidas administrativas aplicables (AD-2) contemplan medias intermedias de seguridad y se contemplan controles mínimos necesarios:

RI 2= Lista de Medidas intermedias de seguridad para accesos desde red interna.
FI 2= Lista de Medidas intermedias de seguridad para accesos físicos.

Las medidas recomendadas contribuyen a la disminución del riesgo que pudiera presentarse en esta Institución.

XII. Técnicas de supresión y borrado seguro de los datos personales

Los datos de carácter personal solo podrán tratarse durante el tiempo **que permanezca vigente**
la finalidad para la que fueron recabados o registrados.

Una vez cumplida la finalidad para la cual fueron recabados los datos personales, las Unidades Administrativas que integran Banjercito deberán cancelar (Eliminación o supresión definitiva).

Previo a la cancelación de los datos personales, las Unidades Administrativas de Banjercito deberán:

a) Identificar los plazos de conservación de los datos personales, o bien, de los documentos y/o expedientes en los que obren los mismos.

b) Asegurarse de que los plazos de conservación atiendan y consideren:

   i. las disposiciones aplicables en la materia de que se trate, y

   ii. los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

c) Observar los plazos de prescripción previstos en la normativa que resulte aplicable o, en su caso, en las cláusulas contractuales, para efectos de las posibles responsabilidades.

La **cancelación (Eliminación o supresión definitiva)** de los datos personales, se realizará tomando en cuenta los plazos de conservación previstos en el Catálogo de Disposición Documental de Banjercito que corresponda, partiendo del momento en que inició el tratamiento de los datos personales y el último uso de los mismos, por lo que una vez que se cumpla la finalidad para la cual fueron recabados y en tanto no se cumpla el plazo de conservación, se llevará a cabo un **bloqueo previo** Durante el periodo de bloqueo, los datos personales no serán objeto de tratamiento, salvo disposición expresa de una ley o que exista una

resolución judicial, orden o mandato, fundado y motivado, de autoridad competente.

El bloqueo de datos personales deberá realizarse tomando en cuenta los medios de almacenamiento físicos y/o electrónicos en los que se encuentran la información.

Cancelación de los datos personales (Eliminación o supresión definitiva)

Vencido el plazo máximo permitido de tratamiento de datos por haber dejado de ser necesarios para la finalidad para la que se recabaron, los datos personales deberán ser **cancelados**, debiendo conservarse **bloqueados** durante el tiempo en el que pueda exigirse algún tipo de responsabilidad derivada de la relación u obligación jurídica, la ejecución de un contrato o la aplicación de medidas precontractuales solicitadas por el interesado, según sea el caso.

Sin perjuicio de analizar en cada caso el tiempo necesario durante el que deben permanecer bloqueados los datos personales, con carácter general se consideran como tiempos de bloque los siguientes:

Datos personales para la gestión de Factor Humano: 1 año, a excepción de los datos personales sobre salarios y cotizaciones que será de 5 años.

Datos personales con fines fiscales: 5 años.

Datos personales para fines contables: 5 años.

Datos de carácter patrimonial: 5 años.

Datos personales relacionados con acciones civiles, penales y administrativas: 5 años.

Datos personales relacionados con acciones reales sobre bienes inmuebles: 35 años.

Datos personales relacionados con la salud: 5 años desde la terminación del proceso asistencial.

La cancelación de los personales se realizará mediante el bloqueo previo, que en función del sistema de tratamiento será:

-Bloqueo lógico: Cuando los datos de carácter personal se encuentren almacenados en aplicaciones o bases de datos ubicadas en sistemas de información.

Este bloqueo previo a la cancelación (supresión definitiva), se solicitará a la Dirección de Tecnologías de la Información y Comunicaciones, vía oficio, adjuntando para tales efectos el **Formulario de solicitud de bloqueo de datos personales**, copiando a el/la Oficial de Protección de Datos Personales de Banjercito, a efecto de que se realice el registro correspondiente y corran los plazos del bloqueo correspondiente:

Formulario de solicitud de bloqueo de datos personales de Banjercito

Procedimiento	Bloqueo de datos personales
Responsable	Titular de la Unidad Administrativa dueña de la aplicación, soporte informático, sistema interinstitucional, o base de datos en la que se encuentran los datos personales a bloquear.
Nombre de la aplicación, sistema o base datos en la que se encuentran los datos personales a bloquear	
Fecha de inicio del bloqueo	
Fecha de terminación del bloqueo	
Fecha en la que se debe hacer efectiva la cancelación (supresión definitiva)	

Bloqueo físico: Cuando los datos personales estén almacenados en soportes físicos o documentos, se procederá a:

a) **Almacenar los soportes en un lugar de acceso restringido**, en cuyo caso, se elaborará un listado de los servidores públicos o personas con acceso autorizado a la ubicación donde se encuentren almacenados, debiéndose llevar un control de acceso por medio de una bitácora que establezca el nombre de los servidores públicos o personas que hayan tenido acceso a los datos personales bloqueados. Debiendo informar de manera trimestral mediante oficio al Oficial de Protección de Datos Personales de Banjercito, a efecto de que este lleve un control puntual de los accesos a datos personales confidenciales y en su caso este en posibilidades de rendir el informe correspondiente a la autoridad.

Transcurrido en cada caso el tiempo de bloqueo de los datos personales se deberá proceder a su
Cancelación (Eliminación o supresión definitiva), salvo que:

a) Se deseen conservar, en cuyo caso, se deberá proceder a su **disociación.**
b) Se destinen a **fines históricos, estadísticos o científicos**, debiendo depurar previamente todos aquellos datos que resulten inadecuados, impertinentes y excesivos para esta nueva finalidad.

Si los datos personales se encuentran almacenados en aplicaciones, bases de datos, soportes informáticos y/o sistemas interinstitucionales, la **cancelación (Eliminación o supresión definitiva)**, en su caso, se solicitará a la Dirección de Tecnologías de la Información y Comunicaciones, vía oficio, adjuntando para tales efectos el **Formulario de solicitud de cancelación de datos personales**, copiando a el/la Oficial de Protección de Datos Personales de Banjercito, a efecto de que se realice el registro correspondiente y corran los plazos del bloqueo correspondiente:

Formulario de solicitud de cancelación de datos personales de Banjercito

Procedimiento	Cancelación (Eliminación o supresión definitiva) de datos personales
Responsable	Titular de la Unidad Administrativa dueña de la aplicación, soporte informático, sistema interinstitucional, o base de datos en la que se encuentran los datos personales a bloquear.
Nombre de la aplicación, sistema o base datos en la que se encuentran los datos personales a bloquear	
Fecha de terminación del bloqueo	
Fecha de cancelación (Eliminación o supresión definitiva)	

Transcurrido el periodo de bloqueo, las Unidades Administrativas de Banjercito deberán realizar la cancelación de los datos personales en la base de datos correspondiente.

La cancelación de los datos personales deberá de ser de forma definitiva, de tal manera que la probabilidad de recuperarlos o reutilizarlos a través de técnicas forenses o de laboratorio sea mínima.

Para la cancelación de los datos personales, las Unidades Administrativas de Banjercito, deberán tomar en cuenta como mínimo lo siguiente:

a) Irreversibilidad: que el proceso utilizado no permita recuperar los datos personales;

b) Seguridad y confidencialidad: que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

c) Favorable al medio ambiente: que el método utilizado produzca el mínimo de emisiones y desperdicios al medio ambiente.

Consideraciones para la cancelación en medios digitales

Las Unidades Administrativas responsable de los datos personales en su posesión, *con apoyo de* la Dirección de Tecnologías de la Información y Comunicaciones, así como de la Subdirección de Seguridad de la Información, deben tener en cuenta las siguientes recomendaciones antes de llevar a cabo la eliminación segura de los datos personales, para determinar el tiempo y los recursos humanos, financieros y técnicos que se invertirán:

a) Identificar el tipo y tamaño del medio de almacenamiento que requiere eliminación segura de datos.
b) Los requerimientos de confidencialidad para los datos almacenados en el medio, de acuerdo al nivel de riesgo de los datos contenidos.

Con base en estos requerimientos, se debe verificar la posibilidad de conocer, de manera anticipada, la cantidad de medios –clasificados por tipo de medios- que serán sometidos a una eliminación segura, con lo cual se debe generar un calendario de eliminación de medios, a través del cual se podrá determinar lo siguiente:

a) La posibilidad de ejecutar la eliminación de la información en un ambiente controlado.

b) La disponibilidad de equipo y herramientas para la eliminación de la información.

c) Si la eliminación de la información puede ser realizada por personal de la Dirección de Tecnologías de la Información y Comunicaciones o se requiere un tercero.

d) El nivel de formación del personal con respecto al equipo/herramientas de eliminación de información.

e) El tiempo requerido para realizar la eliminación de los datos y

f) El costo de la eliminación de los datos en el medio, considerando las herramientas, la capacitación, verificación y su reutilización.

Técnicas de eliminación de datos personales

En medios Digitales.

- **Testar**. Técnica empleada para eliminar partes específicas de un documento digital que evita la visualización de los datos confidenciales durante un proceso de desclasificación. Esta técnica incluye el borrado de metadatos y la eliminación de imágenes y texto.

- **Borrar**. Esta técnica realiza un borrado sencillo que sólo elimina la referencia a los archivos en el sistema operativo (desindexación); los datos continúan en el medio de almacenamiento y éstos pueden ser recuperados aplicando técnicas de cómputo forense.

- **Limpiar**. Emplea procedimientos basados en software para la sobre-escritura de los datos en los medios de almacenamiento con la finalidad de que no puedan ser recuperados a través del uso de técnicas de cómputo forense. Lo anterior puede aplicarse a un archivo específico o el medio completo. Cuando la sobre-escritura no está soportada por el dispositivo, se reinicia con los valores de fábrica. Este método no puede ser utilizado para medios dañados o que no pueden ser sobre-escritos.

- **Purgar**. Emplea técnicas físicas o lógicas que evitan que los datos que contiene el medio sean recuperados empleando técnicas de laboratorio avanzadas. Se recomienda en caso de que el dispositivo sea reutilizado, reciclado o desechado. En esta categoría se encuentran la sobre-escritura, el borrado de bloque, el borrado criptográfico y la des-magnetización.

En medios físicos.

- **Testar**. Aplica a medios físicos escritos. Consiste en el truncamiento de determinadas partes en un documento con la finalidad de prevenir revelaciones de información reservada o confidencial (datos personales).

- **Destruir**. Elimina los datos a través de la destrucción física del medio que los almacena, dejándolos inutilizables. Las técnicas de destrucción son las siguientes:

- **Desintegración, incineración, pulverización, fundición**. Métodos diseñados para destruir de manera definitiva el medio de almacenamiento.

- **Trituración**. Método diseñado para reducir el medio de almacenamiento de tal manera que no pueda ser reconstruido.

Métodos de verificación

La Unidad de Transparencia de Banjercito, previa consulta a la Subdirección de Seguridad de la Información, debe verificar posterior a la eliminación segura de los datos en el medio que la técnica empleada garantice la confidencialidad de los datos eliminados.

Para tal efecto, existen dos métodos de verificación:

- **Completa**. Este método revisa de manera detallada cada dispositivo y garantiza la efectividad de la técnica aplicada en la eliminación segura de los datos. Se debe considerar que su aplicación toma mucho tiempo.

- **Por muestreo**. En este método se toma un subconjunto de los medios a los que se les aplicó la eliminación segura. Se recomienda que se verifiquen al menos el 25% de los dispositivos borrados. Su nivel de detalle es menor y por lo tanto requiere menos tiempo.

Para los datos personales contenidos en medios digitales:

Independientemente de la técnica aplicada en la eliminación de los datos personales las Unidades Administrativas responsables de los datos personales, deben generar un certificado que puede ser tanto un registro electrónico o un documento en papel con, al menos, la siguiente información:

- Datos del medio que contiene los datos personales:
  - Fabricado por / Marca.
  - Modelo.
  - Número de serie.
  - Número de inventario (en caso de que aplique).
- Tipo de medio: impreso, magnético, óptico, electrónico.
- Origen del medio: computadora personal, servidor, teléfono celular, etc.
- Descripción de la técnica de eliminación: limpieza, purga, destrucción.
- Método usado: des-magnetización, sobre-escritura, borrado de bloques, borrado criptográfico, trituración, etc.
- Herramienta utilizada, incluyendo el número de versión.
- Método de verificación.
- Destino del medio posterior a la eliminación segura de la información.
- Respaldo. Indicar si la información se respaldó y de ser así, en dónde.
- Tanto para la eliminación segura y la verificación, incluir:
- Nombre de quien realizó la eliminación
- Nombre de quien validó la eliminación
- Cargo y Área
- Fecha
- Localización
- Teléfono y correo electrónico
- Firma
- Incluir nombre, cargo y firma de quien autoriza la eliminación.

Para los datos personales contenidos en medios impresos:

> Se debe cumplir con lo indicado en los procedimientos de destrucción de documentos (expedientes) establecidos por la Subdirección de Gestión Documental

Selección del método de eliminación basado en el nivel de riesgo
El nivel de riesgo de los datos personales se determina con base a la clasificación del dato personal establecida en el Procedimiento 04 Principios y Deberes de Datos Personales, de este Manual, se describe la categorización de los datos personales y el valor del riesgo asociado.

Una vez identificado el riesgo, el *propietario* de los datos debe seleccionar el método adecuado para eliminar la información contenida en el medio (ver Tabla 1).

Tabla1. Identificación de la técnica de eliminación de datos personales con base en el nivel de riego.

Nivel de riesgo	El medio no permanecerá en Banjercito		El medio permanecerá en Banjercito	
	Reutilizado	No reutilizado	Reutilizado	No reutilizado
Bajo	Purgar	Purgar	Limpiar	Limpiar
Medio	Purgar	Destruir	Purgar	Destruir
Alto	Destruir	Destruir	Purgar	Destruir
Reforzado	Destruir	Destruir	Destruir	Destruir

XIII. Procedimientos de respaldo y recuperación de datos personales

XIV. Gestión de vulneraciones a la seguridad de los datos personales

Un incidente de seguridad de la información que implica una vulneración a la seguridad de los datos personales, es aquel que afecte de manera directa los mismos en cualquier fase de su tratamiento. De acuerdo con el artículo 38 de la LGPDPPSO, se consideran al menos las siguientes vulneraciones:

- La pérdida o destrucción no autorizada.
- El robo, extravío o copia no autorizada.
- El uso, acceso o tratamiento no autorizado
- El daño, la alteración o modificación no autorizada.

Las variables que el Oficial de Protección de Datos Personales tomará en consideración serán los criterios de sensibilidad por dato personal, siendo los siguientes:

NIVEL SENSIBILIDAD

Muy alto: Los datos de mayor riesgo son aquellos que de acuerdo con su naturaleza derivan en mayor beneficio para un atacante en caso de obtenerlos, por ejemplo: información adicional de tarjeta bancaria (fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal PIN).

Alto: Esta categoría de datos contempla a los datos personales sensibles, tales como:

- Datos de salud
- Filosóficas y morales
- Información genética
- Afiliación sindical
- Origen racial o étnico

- Opiniones políticas
- Ideología
- Preferencia sexual
- Creencias religiosas
- Hábitos sexuales
- Cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.

Medio: Se incluyen los datos que permiten conocer la ubicación física de la persona, datos patrimoniales, de autenticación con información referente a los usuarios como son las contraseñas, además se incluye en este rubro la información biométrica, datos jurídicos y de la tarjeta bancaria.

Bajo: Integra los datos de identificación y contacto o información académica o laboral.
La notificación remitida a la Unidad de Transparencia deberá contener al menos, la siguiente información:

- La hora y fecha de la identificación de la vulneración;
- La hora y fecha del inicio de la investigación sobre la vulneración;
- La naturaleza del incidente o vulneración ocurrida;
- La descripción detallada de las circunstancias en torno a la vulneración ocurrida;
- Las categorías y número aproximado de titulares afectados;
- Los sistemas de tratamiento y datos personales comprometidos;
- Las acciones correctivas realizadas de forma inmediata;
- La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;
- El listado de acciones y recomendaciones que puede realizar el titular de los datos personales para minimizar los efectos adversos de la vulneración;
- El medio puesto a disposición del titular para que pueda obtener mayor información al respecto;
- El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar más información al Instituto, en caso de requerirse, así como atender dudas y proporcionar información adicional del incidente.

Asimismo, se adjuntarán para tales efectos los siguientes anexos:

Anexo 1 "Formato de identificación de incidentes
Anexo 2 Formato de investigación del incidente
Anexo 2 Formato de investigación del incidente

- Datos de investigación
- Acciones de contención

- Acciones de mitigación
- Procesamiento de indicios o evidencias
- Acciones de recuperación
  Anexo 3 Formato de recuperación de incidente
  Anexo 4 Copia del CUB – Anexo 64 "Reporte de eventos de Perdida de Información Administrada a través de Medios Electrónicos" y de la información remitida a la CNBV

XIII. Gestión de vulneraciones a la seguridad de los datos personales.

Un incidente de seguridad de la información que implica una vulneración a la seguridad de los datos personales, es aquel que afecte de manera directa los mismos en cualquier fase de su tratamiento. De acuerdo con el artículo 38 de la LGPDPPSO, se consideran al menos las siguientes vulneraciones:

- La pérdida o destrucción no autorizada.
- El robo, extravío o copia no autorizada.
- El uso, acceso o tratamiento no autorizado
- El daño, la alteración o modificación no autorizada.

Las variables que el Oficial de Protección de Datos Personales tomará en consideración serán los criterios de sensibilidad por dato personal, siendo los siguientes:

NIVEL SENSIBILIDAD

Muy alto: Los datos de mayor riesgo son aquellos que de acuerdo con su naturaleza derivan en mayor beneficio para un atacante en caso de obtenerlos, por ejemplo: información adicional de tarjeta bancaria (fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal PIN).

Alto: Esta categoría de datos contempla a los datos personales sensibles, tales como:

- Datos de salud
- Filosóficas y morales
- Información genética
- Afiliación sindical
- Origen racial o étnico
- Opiniones políticas
- Ideología
- Preferencia sexual

- Creencias religiosas
- Hábitos sexuales
- Cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.

Medio: Se incluyen los datos que permiten conocer la ubicación física de la persona, datos patrimoniales, de autenticación con información referente a los usuarios como son las contraseñas, además se incluye en este rubro la información biométrica, datos jurídicos y de la tarjeta bancaria.

Bajo: Integra los datos de identificación y contacto o información académica o laboral.

- La notificación remitida a la Unidad de Transparencia deberá contener al menos, la siguiente información:
- La hora y fecha de la identificación de la vulneración;
- La hora y fecha del inicio de la investigación sobre la vulneración;
- La naturaleza del incidente o vulneración ocurrida;
- La descripción detallada de las circunstancias en torno a la vulneración ocurrida;
- Las categorías y número aproximado de titulares afectados;
- Los sistemas de tratamiento y datos personales comprometidos;
- Las acciones correctivas realizadas de forma inmediata;
- La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;
- El listado de acciones y recomendaciones que puede realizar el titular de los datos personales para minimizar los efectos adversos de la vulneración;
- El medio puesto a disposición del titular para que pueda obtener mayor información al respecto;
- El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar más información al Instituto, en caso de requerirse, así como atender dudas y proporcionar información adicional del incidente.

Asimismo, se adjuntarán para tales efectos los siguientes anexos:

- Anexo 1 "Formato de identificación de incidentes
- Anexo 2 Formato de investigación del incidente
- Datos de investigación
- Acciones de contención
- Acciones de mitigación

- Procesamiento de indicios o evidencias
- Acciones de recuperación
- Anexo 3 Formato de recuperación de incidente
- Anexo 4 Copia del CUB – Anexo 64 "Reporte de eventos de Perdida de Información Administrada a través de Medios Electrónicos" y de la información remitida a la CNBV

XIV. Relación responsable-encargado: Modelo de Anexo de Tratamiento de datos personales

Con la finalidad de dar cumplimiento a lo previsto por el artículo 59 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), se deberán implementar para cualquier contratación institucional que advierta un tratamiento de datos personales, los siguientes formatos:

- Cláusulas de confidencialidad, protección de datos personales, secreto bancario y destino de los datos personales al finalizar el servicio.
-

CONFIDENCIALIDAD

Cláusula ___- **"EL PRESTADOR"** se obliga expresamente a mantener y guardar en estricta y absoluta confidencialidad y reserva toda la información o documentación que le sea proporcionada por **"BANJERCITO"** o de cualquier otra fuente.

PROTECCIÓN DE DATOS PERSONALES

Clausula____- Derivado del presente instrumento **"EL PRESTADOR"** tendrá acceso a Datos Personales, por lo que bajo protesta de decir verdad en el presente acto, se obliga a implementar las medidas de seguridad de carácter administrativo, físico y técnico para su debida protección contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como, garantizar su confidencialidad, integridad y disponibilidad de acuerdo a lo establecido por los artículos 30 y 59 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En caso de que ocurra una vulneración a la seguridad de los datos personales ocurrida en cualquier fase del tratamiento, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales aun cuando ocurra de manera accidental, **"EL PRESTADOR"** notificará a **"BANJERCITO"**, sin dilación alguna.

La notificación que realice **"EL PRESTADOR"** contendrá, al menos, la siguiente información:

a. La naturaleza del incidente.
b. Los datos personales comprometidos.
c. Las acciones correctivas realizadas de forma inmediata.
d. Las recomendaciones sobre las medidas que éste pueda adoptar para proteger sus intereses.
e. Los medios disponibles al titular para obtener mayor información al respecto.

"EL PRESTADOR" documentará toda vulneración de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificando, de manera enunciativa más no limitativa, la fecha en que ocurrió; el motivo de la vulneración; los hechos relacionados con ella y sus efectos y las medidas correctivas implementadas de forma inmediata y definitiva, la cual estará a disposición de **"BANJERCITO"**.

SECRETO BANCARIO

Cláusula___ – **"EL PRESTADOR"** manifiesta que conoce el contenido del artículo 46 bis 1 de la Ley de Instituciones de Crédito (LIC), el cual establece que las personas que contraen con las Instituciones de Crédito, deberán salvaguardar la confidencialidad de la información de los usuarios del sistema bancario y proveer que en la celebración de dichas operaciones se cumplan las disposiciones aplicables para que lleven a cabo servicios necesarios para su operación, les serán aplicables las disposiciones relativas a los secretos bancarios establecidos en el artículo 142 de la LIC, aun cuando dejen de laborar o prestar sus servicios.

DESTINO DE LOS DATOS PERSONALES AL FINALIZAR EL SERVICIO

Es obligación de "LAS PARTES" almacenar la información de _____ por un periodo de 5 años, contados a partir de la fecha de finalización del trámite para fines de cualquier consulta, auditoria o solicitud, en su caso.

Para efectos de la presente cláusula se entenderá por RESPONSABLE a BANJERCITO y por ENCARGADO a (nombre de la empresa).

Al finalizar el servicio, "EL ENCARGADO" cancelará los datos personales que consten digital o analógicamente y una vez efectuado lo anterior remitirá a "EL RESPONSABLE" un oficio de certificación de su destrucción por escrito, en el entendido que "EL ENCARGADO" no podrá bajo ninguna circunstancia retener o conservar la información confidencial o copia de la misma, impresa o electrónica.

Posteriormente, "EL RESPONSABLE", por conducto de la Subdirección de Seguridad de la Información y el Oficial de Protección de Datos Personales

realizará una visita de inspección en las instalaciones de "EL ENCARGADO", para verificar el cumplimiento de lo anterior, por lo que deberá permitirse el acceso al personal descrito, a efecto de realizar la verificación

- Modelo de anexo de tratamiento de datos personales para las contrataciones institucionales.

El citado modelo de anexo se deberá adecuar a las necesidades de cada contratación, en específico para cubrir todos los aspectos de la misma y los relacionados con la protección de los datos personales que se traten.
ANEXO PARA EL TRATAMIENTO DE DATOS PERSONALES QUE CELEBRAN POR UNA PARTE, BANCO NACIONAL DEL EJÉRCITO, FUERZA AÉREA Y ARMADA, SOCIEDAD NACIONAL DE CRÉDITO, INSTITUCIÓN DE BANCA DE DESARROLLO, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ COMO "EL RESPONSABLE", LEGALMENTE REPRESENTADO POR _____, EN SU CARÁCTER DE DIRECTOR GENERAL ADJUNTO DE ADMINISTRACIÓN, Y POR LA OTRA PARTE LA PERSONA MORAL DENOMINADA _____, A QUIEN EN LO SUCESIVO SE DENOMINARÁ COMO "EL ENCARGADO", LEGALMENTE REPRESENTADA POR_____; EN SU CARÁCTER DE REPRESENTANTE LEGAL; DENOMINÁNDOLES DE MANERA CONJUNTA "LAS PARTES"; AL TENOR DE LAS SIGUIENTES:

D E C L A R A C I O N E S

I.Declara "EL RESPONSABLE" a través de su representante, bajo protesta de decir verdad, que:

I.1 Es una Sociedad Nacional de Crédito legalmente constituida conforme a las Leyes de este País, lo que consta en la escritura pública número 56 de fecha 06 de mayo de 1947, otorgada ante la fe del Licenciado Manuel Borja Soriano, titular de la Notaría Pública número 78 de la Ciudad de México, inscrita en el Registro Público de la Propiedad y del Comercio de esta Ciudad de México, el día 12 de junio de 1947, registrado bajo el número 149 a fojas 159, del volumen 231 del libro 3°.

I.2. Su representante, _____, en su carácter de Director _____ y Representante Legal, cuenta con las facultades suficientes para la firma de éste Instrumento, tal y como consta en el Instrumento Notarial N° _____ de fecha _____, otorgado ante la fe del _____, Notario número ___ de la Ciudad de México, facultades que a la fecha no le han sido revocadas, modificadas, ni limitadas en forma alguna.

I.3. El Director/a de, o quien en un futuro la sustituya, se constituye como encargada del seguimiento del presente Convenio, es decir, fungirá como responsable de verificar su debido cumplimiento.

I.4. Para los fines y efectos legales del presente instrumento, señala como domicilio el ubicado en Avenida Industria Militar 1055, Col. Lomas de Sotelo, Miguel Hidalgo, C.P. 11200, de esta Ciudad de México.

I.5. Se encuentra inscrito en el Registro Federal de Contribuyentes con el numero: **BNE820901682.**

II. Declara "EL ENCARGADO", a través de su representante, bajo protesta de decir verdad, que:

II.1. Es una Sociedad _____, legalmente constituida conforme a las Leyes de este País bajo la denominación social de "_____"; lo que se acredita con el Testimonio Notarial de la Escritura Pública número _____ de fecha _____, otorgada ante la fe del C. Lic. _____; Notario Público número_____ de la Ciudad de México, misma que se encuentra inscrita en la Sección de Comercio del Registro Público de la Propiedad de la Ciudad de México , en el libro _____, volumen _____ a fojas _____ y bajo el número _____.

II.2. El **C. Lic.** _____ en su carácter de representante legal, cuenta con las facultades propias y suficientes para la firma del presente Instrumento, mismas que a la fecha no le han sido revocadas, modificadas, ni limitadas en forma alguna, lo que consta en el Testimonio Notarial de la Escritura Pública número _____ de fecha _____, otorgada ante la fe del C. Lic. _____ Notario Público número _____ del _____, misma que se encuentra inscrita en el Registro de Comercio con número de folio mercantil _____, de fecha _____.

II.3 Se encuentra inscrito en el Registro Federal de Contribuyentes número _____.

II.4. Cuenta con los conocimientos, capacidad, experiencia, elementos técnicos, materiales y humanos propios y suficientes para llevar a cabo eficientemente la realización del objeto del presente Convenio, asimismo, manifiesta que conoce el contenido y los requisitos que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como, las demás disposiciones en materia de protección de datos personales, que regulan el presente instrumento.

II.5. Para los fines y efectos legales del presente instrumento, señala como su domicilio el ubicado en

III. Declaran "LAS PARTES", que:

III.1. Celebran el presente Convenio de conformidad con lo establecido en los artículos 1, 3, fracciones IX, XV, XVII y XXVIII, 4,16, 17, 18, 22 fracción II, 31, 32, 33, 38, 58, 59, 60, 61, 62, 63, 64, 65,66, 67, 68, 69, 70 fracciones II y VII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) publicada en el Diario Oficial de la Federación el 26 de enero de 2017.

III.2. Que BANJERCITO, en el carácter de "EL RESPONSABLE" encomienda a "EL ENCARGADO", el tratamiento de datos personales objeto del contrato principal.

III.3. Que "EL RESPONSABLE" ha contratado los servicios de (NOMBRE DE LA PERSONAL MORAL), consistentes en: (INDICAR TIPO DE SERVICIO).

III.4. Que, para el cumplimiento de dichos servicios, a "EL ENCARGADO" le resulta necesario el acceso y tratamiento de los datos personales a nombre y encargo de "EL RESPONSABLE".

III.5. Que en cumplimiento de lo dispuesto en el artículo 59 del LGPDPPSO, "EL ENCARGADO" ofrece suficientes garantías para implementar políticas técnicas y organizativas apropiadas para aplicar las medidas de seguridad de carácter administrativo, físico y técnico para la protección de datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, por lo cual ambas partes convienen suscribir el presente Convenio con sujeción a las siguientes:

CLÁUSULAS

PRIMERA. – DEFINICIONES: Para los efectos del presente Convenio se entenderá por:

Anexo A: Listado de personas autorizadas para accesar y dar tratamiento a los datos personales a cuenta de "**EL ENCARGADO**".

Archivo de transmisión: Conjunto ordenado de datos personales referentes a clientes de **"EL RESPONSABLE"**, sus beneficiarios y/o cotitulares.

Banjercito: Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C.

Bloqueo de datos personales: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento, y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

Cancelación de datos personales: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Contrato Principal: Es aquel que da vida a la prestación del servicio, mediante el cual se da el tratamiento de datos personales.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Responsable: Para efectos del presente, es Banjercito, toda vez que es quien posee la información.

Encargado: La persona física ajena a Banjercito, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta de Banjercito.
Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel

organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Oficio de certificación: Documento por medio del cual, "**EL ENCARGADO**", remite al "**EL RESPONSABLE**" la documentación que acredite los mecanismos que utilizó para la cancelación de datos personales que se le encomendaron.

SEGUNDA. – OBJETO.

El objeto del presente Convenio es **regular las bases y mecanismos para el tratamiento de los datos personales**, que implica el acceso por parte de **"EL ENCARGADO"** a diversa información respecto de clientes titulares, sus beneficiarios y/o cotitulares.

Lo anterior no se considerará, para la presente relación jurídica, como una transferencia de datos ya que dicho tratamiento resulta necesario para consecuir

las finalidades previstas en el Contrato Principal. Es por ello que, para efecto de cumplir con las obligaciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, las personas designadas en el '**ANEXO A**' serán considerada como **"ENCARGADOS DEL TRATAMIENTO"** de los datos personales contenidos en el **"ARCHIVO DE TRANSMISIÓN"**. El tratamiento de datos personales consistirá en el acceso necesario para llevar a cabo el servicio prestado.

TERCERA- TIPO DE DATOS PERSONALES SOMETIDOS AL TRATAMIENTO

"EL ENCARGADO" a nombre y cuenta de "EL RESPOSABLE", en el marco (descripción del contrato o relación jurídica que justifica el tratamiento de datos), autoriza el tratamiento de datos personales contenidos en el "Archivo de Transmisión" (Descripción clara el inventario de datos personales a tratar).

CUARTA. - OBLIGACIONES DE "EL RESPONSABLE"

"EL RESPONSABLE" garantiza que los datos personales otorgados a "EL ENCARGADO", se han obtenido lícitamente y que son adecuados, pertinentes y limitados a los fines del tratamiento.

"EL RESPONSABLE" pondrá a disposición de "EL ENCARGADO" la información necesaria para ejecutar la prestación del servicio objeto del encargo.

"EL RESPONSABLE" advierte a "EL ENCARGADO" que deberá realizar las actividades de tratamiento de datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido de mismo, así como, limitar sus actuaciones a los términos fijados por "EL RESPONSABLE", si determina por su cuenta los fines y los medios del tratamiento, asumirá el carácter de responsable del tratamiento de los datos personales y estará sujeto a cumplir las disposiciones normativas vigentes en la materia que resulten aplicables.
Para el cumplimiento del objeto del presente instrumento, **"EL RESPONSABLE"** se compromete a integrar el **"Archivo de transmisión"**, previa validación de la información para detectar entre otras circunstancias especiales, duplicidades, homonimias, entre otras causas.
Remitir al correo electrónico_____el **"Archivo de transmisión"** dentro de ____días hábiles primeros de cada mes, con las medidas de seguridad mínimas establecidas en el **ANEXO 1A** denominado **"Requerimientos Mínimos de seguridad informática"**
Informar las actualizaciones que sufra la información entregada originalmente, informando, altas y bajas de los mismos, así como la razón de cada uno de los casos, de manera enunciativa mas no limitativa, por causas de defunción,

renuncia, nuevos pensionados o jubilados en los términos del **ANEXO 1A** que forma parte integral del presente Convenio.

QUINTA. - OBLIGACIONES DE "EL ENCARGADO"

"EL ENCARGADO", no destinará, aplicará o utilizará los datos a los que tenga acceso para un fin distinto al encargo o que suponga el incumplimiento de este Convenio.

"EL ENCARGADO" pondrá a disposición de "EL RESPONSABLE" la información necesaria para demostrar el cumplimiento del Contrato Principal, permitiendo las inspecciones y auditorías necesarias para evaluar el tratamiento.

"EL ENCARGADO", se obliga a guardar la confidencialidad de cualquier información que obtenga o se haga de su entero conocimiento, relacionada con los servicios contratados de "_____", por lo que a partir de la fecha de suscripción del presente instrumento, no podrá divulgar esa información, reproducirla o transmitirla por ningún medio a cualquier tercero o al público en general; tampoco podrá resumirla, modificarla o alterarla en forma alguna, ni darle un uso comercial o distinto al autorizado.

En virtud de lo anterior, queda entendido que "EL ENCARGADO" debe asegurarse que cada receptor de información se adhiera al compromiso de confidencialidad previsto en el presente Convenio. Asimismo, "EL ENCARGADO", asume la obligación de no revelar la información confidencial aún después de terminado el Contrato Principal, entendiéndose esta obligación por tiempo indefinido.

"EL ENCARGADO", deberá realizar por escrito, un registro de todas las actividades de tratamiento efectuadas por cuenta propia, mismo que contendrá:

a. El nombre y los datos de contacto de "EL ENCARGADO"
b. Las actividades de tratamientos efectuados,
c. En su caso, las transferencias de datos personales a terceros
d. Una descripción general de las medidas de seguridad de carácter administrativo, físico y técnico relativas a:

i. La disociación y el cifrado de datos personales,
ii. La confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios de tratamiento.
iii. Las directrices para restaurar la disponibilidad a los datos personales de forma rápida, en caso de incidente físico.
iv. Procedimiento de verificación, evaluación y valoración regulares de las medidas de seguridad de carácter

administrativo, físico y técnico para garantizar la seguridad del tratamiento.

SEXTA. - PERSONAL AUTORIZADO PARA REALIZAR EL TRATAMIENTO DE DATOS PERSONALES.

"EL ENCARGADO" garantiza que el personal autorizado para realizar el tratamiento se ha comprometido de forma expresa y por escrito a respetar la confidencialidad de los datos personales.

"EL ENCARGADO" tomará medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales sólo pueda tratarlos siguiendo las instrucciones de **"EL RESPONSABLE"**

"EL ENCARGADO" garantiza que el personal autorizado para realizar el tratamiento ha recibido la formación necesaria para asegurar que no se pondrá en riesgo la protección de datos personales.

SÉPTIMA - SUBCONTRATACIONES

Se autoriza a "**EL ENCARGADO"**, a subcontratar los servicios o medios directamente necesarios con los que son objeto del Contrato Principal, estos deberán ser autorizados previamente por escrito por **"EL RESPONSABLE"** y deberá informarse todos los datos del servidor concretamente subcontratado.
"EL SUBCONTRATISTA", que también tiene la condición de "EL ENCARGADO", está obligado igualmente a cumplir todas las obligaciones establecidas en el presente Convenio, y las instrucciones que dicte "EL RESPONSABLE".

"EL ENCARGADO" deberá formalizar por escrito esta relación, de forma que el nuevo "SUBCONTRATISTA" quede sujeto a las mismas condiciones y con los mismos requisitos formales que "EL ENCARGADO", en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de sus titulares. En el caso de incumplimiento por parte de "EL SUBCONTRATISTA", "EL ENCARGADO", inicial seguirá siendo plenamente responsable ante el cumplimiento de las obligaciones.

OCTAVA. - NOTIFICACIONES DE VULNERACIONES A LA SEGURIDAD DE DATOS PERSONALES

En caso de que ocurra una vulneración a la seguridad de los datos personales ocurrida en cualquier fase del tratamiento, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales aun cuando ocurra de manera accidental, **EL**

ENCARGADO" informará a **"EL RESPONSBLE"** sin dilación alguna, a través de atento oficio, adjuntando la evidencia y toda la información relevante para documentar y comunicar la incidencia, para que éste a su vez notifique el incidente al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y a los titulares afectados de dicho acontecimiento, de modo, tiempo y lugar facilitando como mínimo, la siguiente información:

a) Descripción de la naturaleza de la vulneración de los datos personales, inclusive, cuando sea posible, el número aproximado de titulares de datos personales afectados, y el número aproximado de registros de datos personales afectados.

b) El nombre y los datos de contacto de "EL ENCARGADO" responsable de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Descripción de las posibles consecuencias de la vulneración de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas para poner remedio a la vulneración de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

"EL ENCARGADO" coadyuvará a "EL RESPONSABLE" en la realización de la "Evaluación de impacto" relativa a la protección de datos, cuando proceda.

NOVENA. - "EL ENCARGADO" queda obligado a implementar y observar, como mínimo, las siguientes medidas de seguridad:

- La confidencialidad permanente de los sistemas y servicios de tratamiento de datos personales.

- La disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

- La verificación, evaluación y valoración, de forma regular, la eficacia de las medidas de seguridad de carácter administrativo, físico y técnico implementadas para la seguridad del tratamiento de los datos personales.

- La disociación y cifrado de los datos personales.

DÉCIMA. –DESTINO DE LOS DATOS PERSONALES AL FINALIZAR EL SERVICIO

Al finalizar el servicio, "EL ENCARGADO" cancelará los datos personales que consten digital o analógicamente y una vez efectuado lo anterior remitirá a "EL RESPONSABLE" un oficio de certificación de su destrucción por escrito, en el entendido que "EL ENCARGADO" no podrá bajo ninguna circunstancia retener o conservar la información confidencial o copia de la misma, impresa o electrónica.

Posteriormente, "EL RESPONSABLE", realizará una visita de inspección en las instalaciones de "EL ENCARGADO", para verificar el cumplimiento de lo anterior, por lo que deberá permitirse el acceso al personal de la Subdirección de Tecnología y Seguridad Informática, a efecto de realizar la verificación.

DÉCIMA PRIMERA. - DAÑOS Y PERJUICIOS

"EL ENCARGADO" se obliga a resarcir los daños y perjuicios, que cause con motivo de cualquier violación a las obligaciones establecidas en el presente Convenio, sin perjuicio de cualquier otra responsabilidad administrativa, civil o penal que pudiera resultar por los delitos de revelación de secretos, abuso de confianza o cualquiera otros derivados del incumplimiento, además de las cantidades que se generen por concepto de gastos de abogados y del procedimiento judicial que el titular de la información confidencial tenga que promover en contra del receptor de la misma.

En caso de incumplimiento de "EL ENCARGADO" o de "SUBCONTRATISTAS" que han quedado mencionados en cualquiera de las cláusulas del presente Convenio, "EL RESPONSABLE" tendrá derecho a ejercitar en contra de "EL ENCARGADO" o "SUBCONTRATISTAS", las acciones, reclamaciones, quejas, denuncias y demás acciones judiciales o administrativas que considere procedentes, sin perjuicio de exigir el resarcimiento de daños y perjuicios.

DÉCIMA SEGUNDA. - MODIFICACIONES

El presente Convenio podrá ser modificado o adicionado por voluntad de **"LAS PARTES"**, mediante la firma del Convenio Modificatorio respectivo. Dicho cambio o adición surtirá efectos a partir de la fecha de su firma.

Ninguna declaración verbal de persona alguna, modificará o afectará, la forma y alcance legal de los términos y condiciones estipulados en este Convenio.

DÉCIMA TERCERA. - VIGENCIA

La vigencia del presente instrumento surtirá sus efectos a partir de la fecha de su firma y tendrá una vigencia de___. (Deberá estar vigente, por el mismo periodo del contrato principal)

DÉCIMA CUARTA. - TERMINACIÓN ANTICIPADA

"LAS PARTES" podrán dar por terminado anticipadamente el presente instrumento, cuando la información no sea utilizada para el cumplimiento de su objeto o no se cumpla con la restricción de confidencialidad y no difusión de la información intercambiada; así como por solicitud expresa de cualquiera de **"LAS PARTES"**, con una antelación de 30 días naturales, para lo cual bastará motivar la solicitud por escrito y, una vez transcurrido el plazo citado, se tendrá por terminado el Convenio.

DÉCIMA QUINTA. - COMUNICACIONES Y NOTIFICACIONES

Cualquier comunicación o notificación que sea proporcionada de conformidad con el presente Convenio, deberá realizarse por escrito y entregada en los domicilios especificados en el apartado de Declaraciones del Contrato Principal.

"LAS PARTES", considerándose realizadas en la fecha señalada en el acuse de recibo. En el caso de que cualquiera de las partes cambiará su domicilio deberá notificarlo a la otra parte, en los domicilios estipulados en el Contrato Principal con acuses de recibo para los efectos conducentes.

DÉCIMA SEXTA. - Las partes convienen en que intentarán resolver de común acuerdo, aquellas situaciones no previstas en el presente Convenio, quedando entendido que la(s) resolución(es) que se adopte(n) sobre el particular, deberá(n) constar por escrito y firmada(s) por ambas partes.

DÉCIMA SÉPTIMA. – INTERPRETACIÓN, EJECUCIÓN Y CUMPLIMIENTO

Para la interpretación, ejecución y cumplimiento del presente Convenio, las partes se someten expresamente a la legislación, jurisdicción y competencia de los tribunales de la Ciudad de México, renunciando desde este momento a cualquier otro fuero que, por razón de sus domicilios presentes o futuros llegare a corresponderles.

HABIENDO LEÍDO Y ESTANDO DE ACUERDO EN EL CONTENIDO DEL PRESENTE CONVENIO, LIBRE DE DOLO, ERROR O MALA FE, MISMO QUE CONSTA DE 09 (NUEVE) FOJAS ÚTILES ESCRITAS POR UN SOLO LADO, LO RATIFICAN Y FIRMAN POR DUPLICADO EN LA CIUDAD DE MÉXICO, A _____, DÍA DEL MES DE _____ DE 20___ QUEDANDO UN EJEMPLAR EN PODER DE "EL RESPONSABLE" Y UN EJEMPLAR EN PODER DE "EL ENCARGADO".

XV. Funciones del Oficial de Protección de Datos Personales de Banjercito

Con fundamento en al artículo 85, penúltimo párrafo de la LGPDPPSO, el Director General de Banjercito realizará la designación como Oficial de Protección de Datos Personales al servidor o servidora pública que ejerza la Jefatura de Protección de Datos Personales de la Unidad de Transparencia, quien contará con las siguientes funciones:

1. Monitorear los avances o cambios normativos en materia de privacidad y protección de datos personales que pudieran impactar en los ejes rectores y acciones desarrolladas en este tema al interior de Banjercito, haciendo las adecuaciones necesarias.

2. Diseñar y ejecutar una política y/o prácticas de protección de datos personales al interior de Banjercito, o bien, adecuar y mejorar las prácticas ya existentes en el marco de la normatividad aplicable en la materia.

3. Desarrollar un mecanismo para evaluar la eficacia y eficiencia de la política de protección de datos personales de Banjercito.

4. Monitorear y evaluar los procesos internos de la organización vinculados con la obtención, uso, explotación, conservación, aprovechamiento, cancelación y transferencia de datos personales, a fin de asegurar que la información sea protegida, tratada conforme a la normatividad aplicable.

5. Colaborar y coordinar acciones con otras áreas de Banjercito, a efecto de asegurar el debido cumplimiento de la política y/o prácticas de privacidad en sus procesos internos, formatos, avisos, recursos y gestiones que se lleven a cabo.

6. Difundir y comunicar la política y/o prácticas de protección de datos personales implementadas al interior de la organización, así como capacitar a todo el personal sobre las mismas.

7. Fomentar una cultura de protección de datos personales orientada a elevar el nivel de concienciación del personal y terceros involucrados, como encargados, en el tratamiento de datos personales.

8. Identificar e implementar mejores prácticas relacionadas con la protección de datos personales.

XVI. Mecanismos de monitoreo y revisión de las medidas de seguridad de los datos personales.

Entre los mecanismos que se deben adoptar para cumplir con el principio de responsabilidad el artículo 30, fracción V, de la Ley General de Datos Personales en Posesión de Sujetos Obligados (Ley General), establece que se deberá mantener un sistema de supervisión y vigilancia, **incluyendo auditorías**, que permita comprobar el cumplimiento de las políticas de datos personales.

El artículo 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales), dispone que además del monitoreo y supervisión periódica de las medidas de seguridad, se deberá contar con un **programa de auditoría** para revisar la eficacia y eficiencia del sistema de gestión.

Por tanto, con la finalidad de comprobar el cumplimiento de las políticas de protección de datos personales, así como para monitorear y revisar la eficacia y eficiencia del sistema de gestión de seguridad de los datos personales de Banjercito, se prevé la ejecución de auditorías en la materia por parte de la Unidad de Transparencia por conducto del Oficial de Protección de Datos, de conformidad con el programa anual aprobado por el H. Comité de Transparencia, cuyos objetivos serán los siguientes:

Objetivos

-Determinar que los tratamientos de datos personales se encuentren apegados a la normativa aplicable.
-Supervisar la adopción y cumplimiento de las políticas, procedimientos y mecanismos determinados en el Sistema de Gestión de seguridad de los datos personales y el Documento de Seguridad de Banjercito.
-Verificar en conjunto con la Subdirección de Seguridad de la Información y Seguridad Institucional, la eficiencia de las medidas de seguridad físicas, administrativas y técnicas instauradas.
-Validar el avance de los objetivos planteados en el Plan de Trabajo de medidas de seguridad faltantes.
-Prevenir la materialización de vulneraciones a la seguridad de los datos personales.
-Promover la implementación de mejoras en el tratamiento de los datos personales, que permitan elevar su grado de protección.

Cumplimiento de observaciones y requerimientos del Oficial de Protección de datos personales de Banjercito

La Unidad Administrativa auditada deberá remitir por oficio al Oficial de Protección de Datos Personales de Banjercito las evidencias del cumplimiento de las observaciones y requerimientos que le hubieran sido realizados.

Tales evidencias serán examinadas a efecto de dilucidar si cumplen con los extremos determinados y con ello, se atendió la deficiencia, desviación o mejora en el tratamiento de los datos personales.

Si de su examen el Oficial de Protección de Datos Personales corrobora que han sido adecuadamente cumplidas las observaciones y requerimientos, se procederá al cierre de la auditoría.

Por el contrario, de concluir que existen extremos no cumplidos total o parcialmente, el Oficial de Protección de Datos de Banjercito, realizará un único requerimiento adicional, reiterando la forma en que la instancia auditada debe demostrar su acatamiento.

Si a pesar de ello persiste el incumplimiento, el Oficial de Protección de Datos Personales hará constar la persistencia de la deficiencia o desviación y procederá al cierre de la auditoría.

Informe de cierre de la auditoría

Teniendo a la vista la documentación generada en las etapas de la auditoría, la minuta de la reunión final y las evidencias que deriven del cumplimiento de observaciones y requerimientos, el Oficial de Protección de Datos Personales elaborará un **informe final** con el cual se dará por concluida la auditoría y/o realizará la notificación al Director General de Banjercito de las deficiencias o desviaciones detectadas, a efecto de que este ordene la firma de la **Cédula de aceptación del riesgo** y notificará al Comité de Transparencia, para que por su conducto se de vista Órgano Interno de Control para la investigación de una presunta irregularidad respecto de determinado tratamiento de datos personales, en términos del artículo 84, fracción VIII de la LGPDPPSO.
El presente procedimiento tiene como objetivos:

XVII. Sanciones aplicables

Respecto a la seguridad de los datos personales, resulta necesario destacar que el artículo 163 de la LGPDPPSO estipula que **serán causas de sanción** por incumplimiento de las obligaciones establecidas, las siguientes:

-Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.
-Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la LGPDPPSO.
-No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO.
-Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la LGPDPPSO.
-Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO.
-Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la LGPDPPSO.

Las Unidades Administrativas de Banjercito deberán **notificar de manera inmediata al Órgano Interno de Control con copia de conocimiento a la Unidad de Transparencia**, las presuntas irregularidades respecto del tratamiento de datos de que se trate.